2011-7

An Investigation of Data Protection and Computer Security in Small Irish Medical Practices

Sean McGrath
Technological University Dublin, seanc.mcgrath@gmail.com

An Investigation of Data Protection and Computer Security in small Irish Medical Practices

Sean McGrath

A dissertation submitted in partial fulfilment of the requirements of
Dublin Institute of Technology for the degree of
M.Sc. in Computing (Information Technology)

July 2011

I certify that this dissertation which I now submit for examination for the award of MSc in Computing (Knowledge Management), is entirely my own work and has not been taken from the work of others save and to the extent that such work has been cited and acknowledged within the test of my work.

This dissertation was prepared according to the regulations for postgraduate study of the Dublin Institute of Technology and has not been submitted in whole or part for an award in any other Institute or University.

The work reported on in this dissertation conforms to the principles and requirements of the Institute's guidelines for ethics in research.

Signed: _____

Date: ***15 July 2011***

ABSTRACT

Small medical practices store and process the health information of their patients in order to aid in providing care to them. Because of this a level of trust exists between the patients and the practice to ensure the sensitive medical data is kept private and secure. There was no formalised way to test if this trust was well deserved and what level of protection was applied to such sensitive health records. A security model that is applicable to small medical practices for the purpose of protecting and securing the personal health information they store was constructed and validated by a security expert from the security industry. This model was then applied to a number of small medical practices to assess the level of data protection and computer security of medical information present in the surveyed practices. In general the practices were found to be complying with the security model, some discrepancies were discovered and noted. A formalised way to test if the trust patients place in their medical practices is well deserved now exists. The trust that the patients of the small medical practices surveyed placed in their practices was well deserved.

Key words: Data Protection, Computer Security, Security Modelling, Small Medical Practices, Personal Health Information and Records, Health Information Systems,
list 5 to 8 words

ACKNOWLEDGEMENTS

These acknowledgement pages are the most important of this document, I wrote the words in this dissertation but many others have contributed to it and it is only because of these people, to whom I am eternally indebted, that this document exists.

First and foremost Dr Susan McKeever, my supervisor, fortune smiled on me when I was assigned Susan, (but not on Susan by being lumbered with my project), and I was lucky to have a supervisor of such dedication and competence, without whom this project simply would not have happened. If this document means anything she deserves the credit, not the author. Any mistakes are the authors, probably because I didn't listen and left everything too late. Thank you from the bottom of my heart Susan.

All the staff of the School of Computing in DIT, but particularly Damian Gordon for his enthusiasm and love of inspiring others to learn which has helped motivate all whom have been fortunate enough to pass through his classes. Also Fred Mtenzi and his security mind for teaching that security is a way of thinking, among other things.

The only reason that this project is valid from a security point of view is because people with real mastery of the area Darren Fitzpatrick, facilitated by Dermot O'Brien, both of Espion Intelligence[1], were good enough to take the time to review it and tell me what I had done wrong. Their responsiveness and helpfulness will never be forgotten.

The Small Medical Practices I interviewed, for obvious reasons I am unable to name them, but their openness, kindness and willingness to assist and answer questions was very much appreciated, refreshingly honest and crucial to the completion of this project.

My Parents, my rock's in stormy weather, I did the job put in front of me only because of their example and the way they brought me up. I am fortunate to have them and can

[1] Espion Intelligence, http://espion.ie/, last accessed 10th of July 2011.

never thank them enough for all they have done for me. This document is dedicated to them.

My friends, Conor Tolan, Maurice Fallon and Mike Keenan, who travelled this path before and showed me that there is a light at the end of the tunnel. Also my peers from the course whom I was lucky to study this course with and call my friends, Andrew Doggett, Eoin Keating, Pawel Kotarba, Mojtaba Akbari and Tomas Valko, who I shared many coffee's and much conversation and inspiration with. But in particular Bernie Foley and Killian Bannon who wrote their dissertations at the same time as I did, their example and counsel were crucial to the completion of this document.

A quick note on words from Terry Pratchett as this document has many of them:

> "*Words turn us from monkeys into men. We make them, change them, chase them around, we eat them and live by them. They are the workhorses carrying any burden and their usage is the skill of the authors trade and hugely versatile. There are times that the wrong word is the right word and times when words can be manipulated so silence shouts*"
>
> Sir Terry Pratchett, (2010)[2]

Any errors or omissions are solely my own fault.

Thank you, one and all.

Sean McGrath

[2] Professor Sir Terry Pratchett joins Trinity College Dublin, http://www.tcd.ie/Communications/news/pressreleases/pressRelease.php?headerID=1604&pressReleaseArchive=2011, last accessed 10th of July 2011.

TABLE OF CONTENTS

TABLE OF FIGURES

1. INTRODUCTION

1.1 Introduction to the project

Increasingly large amounts of personal and private medical data are being stored and transmitted in and through electronic systems in medical practices such as small General Practitioners Surgeries. This has serious data protection ramifications as such information is regarded as particularly sensitive when stored in systems that keep electronic health records. Health data is defined as:

> "*Sensitive personal data" means personal data as to… (c) the physical or mental health or condition or sexual life of the data subject*"
>
> The DATA PROTECTION ACT, (1988), Section 1. (1) (C).

There are other terms for such medical data, including PHI, Protected Health Information, which is defined under the Health Information and Portability and Accountability Act, (HIPAA), as follows:

> "*PHI is individually identifiable health information that is transmitted or maintained in any form or medium (e.g., electronic, paper, or oral), but excludes certain educational records and employment records*"
>
> Centre for Disease Control and Prevention. (2003)

PHI can also be taken to refer to Personal Health Information, which is essentially the same as protected health information and medical data but, Personal Health Information is a more common European and Irish term as opposed to the American term of Protected Health Information. For the purposes of this project the two are taken to be the same thing.

This project examines the level of data security and protection in small medical practices. A security model suitable for the small medical practices will be established

and this will be used as the foundation for assessing the level of data security and protection in the surveyed small medical practices.

Non technical users of GPs' IT systems may not be aware that these systems should be secure, how they should be secured or why they should be secured. Walsh, (2010), points to "*folk model's*" that users use to secure their home computers and the flaws that they contain. There is a perception of "bad" things and people on the Internet, which can cause harm to a person's computer or to the person themselves through theft, but these are perceptions as opposed to concrete understandings. It is reasonable to assume that users of computing systems in small medical practices who are not technical experts in the field of computing or computer security may apply similar "*folk models*" to the security of the systems that they use if they are responsible for securing them or have any ability to do so, i.e. administrative privileges to their workstations. This has the potential to expose any data on those systems, including Protected Health Information, (PHI), to the risk of compromise as the "*folk model's*" the users may use can allow them to justify ignoring best practice security advice.

In order to understand the problem domain it is necessary to understand the core concepts of computer security, Stoneburner, (2001), lists the objectives of computer security as:

1. Availability
2. Integrity
3. Confidentiality
4. Accountability
5. Assurance

The most important of those from the perspective of PHI and health data in small medical practices is confidentiality. Confidentiality of that information is paramount, for instance Whiddet, et al, (2005) identified significant reluctance amongst patients to share sensitive information with receptionists and managers when dealing with medical information.

This project will attempt to better understand the state of confidentiality, availability, integrity, assurance and accountability in the surveyed small medical practices.

1.2 Background

The place for health data that small medical practitioners store and process is in the wider context of computer and data security. The over-riding objective of this project is in relation to data protection and computer security in small medical practices, but these goals cannot exist in a stand-alone context as that would limit the understanding of the problem domain and thus it is necessary to draw from other sources and areas, such as protections applied to normal information technology assets and other best practices.

The global security arena has experienced a number of high profile security incidents, such as the attack on Sony's Playstation network that exposed the user data of millions of users, Goodin, (2011). In Drummond, (2010), Google outlined the attack that emanated against them from China which stole intellectual property from their network. The Anonymous group unsuccessfully attempted to launch a distributed denial of service attack against Amazon but was more successful against PayPal, Vijayan, (2010).

Incidents like these can have a bearing for the future in small medical practices, they may not have experienced similar attacks at this stage but there is potential for such in the future and thus guidance is needed now. For example the Sony attack happened because of poor procedures for patching the Apache webserver's running the Sony network and a lack of firewalls between the webserver and the internet. Those were costly mistakes, but mistakes that are easy to replicate by anyone.

Also, it is necessary to take into consideration from the forthcoming Health Information Bill that it is expected that even more health data will be stored electronically so health information can be better utilised to provide better health care to the public.

> "*It is widely recognized, however, that it, [Health Data], can have other positive uses that would benefit the health system as a whole in facilitating better planning, management and delivery of services*"

Department of Health and Children (2008, p. 2)

Further one of the goals of the HIB is to:

> "*Protect the privacy, confidentiality, security and integrity of personal health information and ensure that these principles apply explicitly to all persons (and not just clinicians) who have a legitimate reason, in certain situations, to be involved with or access such information: for example, medical students, healthcare administrative personnel, software and hardware vendors who supply and maintain health information systems;"*
>
> Department of Health and Children, (2008, p. 12)

It is in this context that this project intends to provide a mechanism by which the protection offered to such important data can be evaluated.

A friend of the author visited their General Practitioner and noted how the person working at reception, who was not a medical practitioner, had full access to the paper based health records for all the patients of the practice. This was needed to facilitate the member of staff being able to do their job but the question as to the appropriateness of that was still valid.

This prompted some debate as to the level of computer security and data protection of the health records in such practices. Mearian, (2011), cites a survey that found that "*30% of doctors lack basic anti-virus software and 34% do not have network firewalls in place*". These are worrying statistics especially when other anecdotal evidence is examined, Irish Health, (2010), point out how the Data Protection Commissioner of Ireland advised the Health Service Executive to improve data security in it s 2010 annual report. Further evidence from Irish Health, (2008), and Irish Health, (2009), report data breaches of health related information.

Other similar incidents relating to taped backup and data transfers can be cited, Fonseca, (2008), where 2 million health records were exposed when backup tapes were stolen, a similar story in the Irish Times (2009), when another data tape containing

medical records was lost when being transferred from a medical surgery. The BBC in (BBC, 2008) reported a case where again a surgery had a backup tape stolen.

Studies have been conducted into data breaches that have compromised sensitive health information and there is considerable anecdotal and widely reported evidence of sensitive health data being lost.

> "*In the case of Isis Machado mentioned earlier, she was charged and fined under HIPAA for disclosing individually identifiable medical records*"
>
> Johnson, (2009)

> "*One GP downloaded a complete patient database, including the medical histories of 10,000 people, on to an unsecured laptop. The laptop was then stolen from his home and never retrieved*"
>
> Savage, (2009)

However, historically we have not done well protecting this data and studies have called for more stringent protections for it:

> *"Health-care providers and insurers must enact better monitoring and information controls to detect and stop leaks. Information access within many healthcare systems is lax*"
>
> Johnson, (2009)

1.3 Research problem

With the advent of digitalisation of office records, including patient health records GP's no longer keep just paper records of ailments and illnesses of the patients who he or she tended to. Even with a paper based records model there was a risk of un-authorised persons gaining access to that extremely sensitive and confidential information, but that risk was mitigated through the securing of the paper files in a

filing cabinet in a locked office and building. This security model is also relatively easy to understand, keep the doors locked and only give a key to a person who should have access.

Now though such information is stored in electronic format over a myriad of storage and processing options, a local file server or fully externally and possibly internationally hosted software as a service application. Further the data has spread throughout other applications and media. A doctor or care worker can now copy and paste a patients information from an electronic health information system into their email client and send themselves an email to work on from home later. Alternatively they may store such records on a memory stick or laptop computer and remove it from the environments of the surgery.

Where previously a file was one physical object, which if taken from its primary storage location its removal could be noticed. Now though, because of the ease of manipulation of electronic data taking a copy of information is no longer as easy to notice. In addition, where the previous security mechanisms and models of locked keys were easy to understand by non-expert people in the field of Information and Communications Technology, any current model, if there is one, is less easy for a lay person to understand. It would not be possible to completely reduce the complexity of such a model of protection of complicated inter dependent and co dependent systems and processes to the state where a person who is not an expert in the field can immediately grasp the nature of such difficult concepts as public, private key encryption and authorization and access controls.

However, the important people who harness and manipulate the data can and need to be aided in understanding the complex eco system that the data resides in and a guide to the successfulness of their organisations attempts to protect that confidential data can be provided. In essence, that is one of the aims of this project, to increase understanding of the importance of computer security and data protection for small medical practices, making it a less difficult to understand quagmire to the people that walk through it every day and to be able to estimate the current state of protection offered at the surveyed practices.

The secondary research for this project was unable to find evidence if an assessment of the level of data protection applied to health information in small medical practices in Ireland or anywhere else has been carried out. This leads to issues for planning what if, anything, needs to be done to improve on the current situation. The author has been unable to determine if an assessment of the current level of data protection for personal health information on the ground, so to speak, has been carried out in Ireland or elsewhere. It is not possible at this stage to ascertain if the practices used to protect personal health information in Ireland are adequate. Thus there is no "base level" of the protection and security of PHI or a way to accurate assesses that level. The protection of

> "*Designers of military and banking systems can refer to Bell & LaPadula (1973) and Clark & Wilson (1987) respectively, but there is no comparable security policy model that spells out clear and concise access rules for clinical information systems*"
>
> Anderson, (1996, p.1)

1.4 Intellectual challenge

The intellectual challenges of this project span many areas.

- Data Protection Legislation and governance
- Security issues and methods specifically tailored for systems that deal with PHI
- General security concepts applicable to any organisation
- Understanding the common factors and components of the systems used in small medical practices
- The limitations and resource difficulties of the small medical practices themselves

- The conceptual effort to create a security model that is applicable to such environments and being able to apply it to them adequately

The data security and protection model has is somewhat novel, it is implementing procedures and practices that are common in small and medium sized offices around the world to protect their assets, but doing so from a unique perspective that aides in the understanding and assessment of data security and protection measures. Small medical practices operate in those types of environments yet the data they store on their customers is potentially very sensitive and damaging should it be lost. A way of being able to understand the systems and procedures in their environment is required and in order to do that a design is required that can be used as a controlled base to measure against.

1.5 Research objectives

The aim of this project is to construct a valid security model that can be used to assess the state of data protection and computer security in small medical practices. The model will then be applied to a sample of such practices in order to understand the level of protection in those practices.

The following were the objectives for this project:

1. Perform a literature review on data protection legislation

2. Perform a literature review on security matters for specifically PHI related systems as well as a more general review for more common security matters

3. Create a security model applicable to and appropriate for small medical practices

4. Test the security model to ensure its correctness for the problem domain. This test was to be performed by an external security expert

5. Test the model in a selection of small medical practices to determine the level of data security and protection therein and also the level of appropriateness of implementation of the model within the medical practice

6. Evaluate the results of the tests to determine the level of data security and protection in the surveyed medical practices, the correctness of the model for the problem domain and the ease of applicability of the model in the practices.

1.6 Research methodology

Both primary and secondary research was performed for this project.

The primary research involved formal, structured interviews with stakeholders in small medical practices to ascertain the level of data security and protection in their practice. Also feedback was sought from an expert in the field of computer security to ascertain the validity of the constructed computer security model.

The secondary research involved a literature review of material that would assist in meeting the objectives of the project. The material covered was

- The regulatory framework provided by Irish and European Data Protection Legislation. What legislation and directives are in place and the requirements they place on data controllers

- Computer security applied specifically to software and systems that store and processes PHI directly

- Computer security applied to the more general security field for software and systems that may not directly store and processes PHI but may process it in a transient manner, e.g. network traffic or for systems that may deal with related meta data, e.g. file servers that store copies of letters sent to patients that may contain PHI

The results of the literature review and the constructed data security and protection model for small medical practices were used in the primary research. Resources
The following resources are required to complete the project.

- Access to stakeholders in small medical practices who have the necessary information in regards the systems and procedures in place around data security and protection

- Access to a security expert to review and assess the security and data protection framework designed for application to small medical practices

- Access to dissertation supervisor is essential for both guidance and quality control purposes

- Access to Library resources, both printed and electronic for research purposes

- Personal computing equipment and internet access

1.7 Scope and limitations

The scope of this project will be specifically focus to the 4th rule of the Data Protection Commissioner, (n.d.), 8 rules for data protection, the rule to keep the personal data safe and secure. This will apply to the systems and procedures that control the personal health information and how it is accessed and processed. The other rules of data protection are also important however and they will feature in the overall design of the security model, a particular focus is placed on data protection governance in chapter two to aide this.

The approach being taken for this project is limited to the personal health information and health data that small medical practices store and process, other sensitive information such as financial data will not be directly considered. Also, only systems and procedures that interact directly with personal health information will be examined. That will include networks and systems that may not be direct processors of

personal health information but if such information passes through them, such as networks and email services will be considered.

Larger medical practices such as hospitals or large surgeries will not be examined as part of this project.

1.8 Organisation of the dissertation

Chapter two introduces the reader to the regulatory framework around PHI. It examines Irish Data Protection Law and its European counterparts. The intention is to provide the legal basis for which the need for compliance with data protection law is required and to aide in understanding what has to be achieved by this.

Chapter three examines the state of the art in regards security for PHI. It is subdivided into two streams. The first, which examines the concepts behind secure systems designed specifically to deal with PHI, e.g. Health Information Systems and Electronic Health Record Systems. This forms part of the basis to assist in evaluating the state of data security and protection of PHI in small medical practices from the perspective of the software that processes the health information. The second stream deals with the more general field of system and network security of small office and home office environments. This perspective is important as such environments are similar to those deployed in small medical practices and which then process and transfer the PHI.

Chapter four constructs a security model based on the findings of the proceeding chapters as well as industry best practices and guidelines for small medical practices. This model will be used to assess the state of data security and protection in a small medical practice.

Chapter five assesses the constructed security model. The model is assessed from the perspective of its correctness to achieve its aim of ensuring the security for the environment to which it will be applied. An external security expert will conduct this part of the assessment. Chapter five also deals with bringing the security model to the surveyed small medical practices. Chapter five deals with the results of the assessment

the practices compared to the security model and evaluates them to determine the level of data security in the assessed small medical practices.

Chapter six draws conclusions and makes recommendations for future works.

2 DATA PROTECTION LEGSILATION AND GOVERNANCE

2.1 Introduction

Small medical practices deal with the protected health information, (PHI), and medical data or their patients in order to provide the services that their patients require. Dealing with such information is a trade-off, it provides a benefit of more efficiently being able to treat their patients but it also places a burden of protection upon the small medical practices to ensure that the personal health information and medical data is protected.

This chapter will outline the legislative and governance matters that small medical practices in Ireland will face when dealing with protected health information and medical data.

2.2 Data Protection Legislation overview

The primary legislative framework and guidance that small medical practices operate under with regards to the protection of the personal and private data which they collect and process is the Data Protection Act, (1988) and Data Protection (Amendment), (2003). In addition to this EU Directive 95/46 (Data Protection) has had an impact on the formulation of such policy because it deals in depth with the matter of Data Protection and Data Protection legislation harmonisation across the union. There are in addition other policy instruments from the European Commission and Council of Europe that have an impact on data protection and the protection of health information in particular. This section will focus on this legislative framework.

As mentioned there are a number of policy instruments in place for the area of data protection of small medical practices in Ireland and the wider area of Europe as a whole, more will be expanded upon further in this chapter. There are also legislative frameworks that do not apply to Irish and European small medical practices due to the practices not being governed by the jurisdiction of the legislative frameworks.

These include the Health Insurance Portability and Accountability Act, (1996), HIPAA for short, which is a specifically health data legislative tool in the United States that mandates both a security rule and privacy rule for the sensitive data that the Act governs. The privacy rule controls how PHI can be used and disclosed, (Department of Health and Human Services, 2010). While the security rule prescribes the safeguards that should be put in place to maintain the privacy of specifically electronically stored PHI (Department of Health and Human Service, 2003). It tiers the security safeguards into three area', administrative safeguards, physical safeguards and technical safeguards. Within each of these areas a number of criteria and standards are required to protect the PHI that the covered entity may posses.

The HIPAA is not however without its detractors, it has been argued how a lack of technical granularity in HIPAA undermines the right of the patient to privacy due to the generalised nature of the standards used in HIPAA, because the specifics of how to achieve the aim are not provided, privacy is damaged because of such, (Wafa, 2010). As Wafa puts it,

> "*providers are free to deploy solutions, which may be cost-effective, but are outdated or unsound, thereby giving a false impression that they have secured protected health information*"
>
> Wafa, (2010)

This is an interesting point and the paper goes on to further argue that the lack of specific instructions in the area of encryption puts health data at risk as the "*drafters in their definition have nurtured a confusing, divisive, duplicative, and obscenest environment*", (Wafa, 2010). This is a similar point that section 2.4 of this chapter will approach from the perspective of Irish and European legislation, but a different conclusion will be reached.

It should be noted that the research and context for this project takes place in Ireland, hence the focus will primarily be upon Irish and European statutory instruments,

however the addition of other jurisdictions legislative and governance polices on data protection, particularly of health information, will be of assistance at stages.

2.3 Data protection legislation in Ireland

There are a number of definitions and terms the understanding of which are important in the context of this study. The Data Protection Commissioner's document: Data Protection Acts 1988 and 2003 A Guide For Data Controllers, (Data Protection Commissioner, 2011), provides a very useful list of definitions, and is the most clear and helpful that could be found for the purposes of this study. The terms and definitions from this document are reproduced in appendix item A so they may be understood when they are used further in this document.

The Data Protection Commissioner has also outlined 8 rules that must be adhered to when processing personal data.

1. *Obtain and process information fairly*
2. *Keep it only for one or more specified, explicit and lawful purposes*
3. *Use and disclose it only in ways compatible with these purposes*
4. *Keep it safe and secure*
5. *Keep it accurate, complete and up-to-date*
6. *Ensure that it is adequate, relevant and not excessive*
7. *Retain it for no longer than is necessary for the purpose or purposes*
8. *Give a copy of his/her personal data to an individual, on request*

Data Protection Acts 1988 and 2003 A Guide For Data Controllers, (2011)

The Data Protection Commissioner also states:

> "*Access to any personal data within an organisation to be restricted to authorised staff on a 'need-to-know' basis in accordance with a defined policy*"
>
> *Data Protection Acts 1988 and 2003 A Guide For Data Controllers, (2011)*

This is of particular importance for small medical practices where distinctions between the levels of access that different staff should have may not be well defined. The question must be asked, should a secretary or member of staff who is a receptionist needs direct access to patient health information have access to patient private health information and what internal governance is required by small medical practices?

2.3.1 Status of health data for data protection matters

The difficulty of understanding this field by small medical practices is compounded because health information is regarded as being especially sensitive under the framework and the Data Protection (Amendment), 2003, defines sensitive personal data to include data about a data subject's health.

> "*'sensitive personal data' means personal data as to—... the physical or mental health or condition or sexual life of the data subject*"
>
> *Data Protection (Amendment), 2003*

In fact the directive completely exclude's the processing of health information except under certain specific circumstances

> "*The processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and of data concerning health or sex life, are prohibited*"
>
> *EU Directive 95/46 (Data Protection)*

Except under the following circumstances

> "*required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy*"

EU Directive 95/46 (Data Protection)

2.3.2 Small Medical Practice internal governance structures

The concept of internal governance is supported by The Irish College of General Practitioners and the National General Practice Information Technology Group, (2003), which, when discussing an information management document for medical practices states: "*Appropriate arrangements should also be in place to govern access by administrative staff in fulfilment of their duties within the team*".

Further stimulus for this concept is added:

> "*Controllers of medical files should, in accordance with domestic law, draw up appropriate internal regulations which respect the related principles in this recommendation*"
>
> Council of Europe, Committee of Ministers. Recommendation No. R (97) 5 of the Committee of Ministers to Member States on the Protection of Medical Data.

In addition to this the recommendation there is impetuous to have a sole individual formally appointed with responsibility for the security of the information systems and data protection where such system pertains to medical data.

There is further impetuous to consider the control of access to medical data within a small medical practice and to formalize the process by which such access is granted.

> "*Access to any personal data within an organisation to be restricted to authorised staff on a 'need-to-know' basis in accordance with a defined policy*"
>
> Data Protection Commissioner, (Unknown).

Responsibilities are thus placed upon small medical practices in relation to the PHI and medical data that they store and process. It would be recommended that such practices have formalized information and data protection policy document for internal governance purposes that encompasses such matters.

2.3.3 Staff training and contractual requirements

When discussing an information policy document it is recommended:

> *"that it include specific provision for staff training and education in relation to data protection law and confidentiality"* (When talking about an information policy document)
>
> The Irish College of General Practitioners and the National General Practice Information Technology Group, (2003)

The training of staff in relation to data protection concerns of medical data and PHI in small medical practices is a matter to take seriously. With the access that staff have to the sensitive personal health information that resides within small medical practices there is need for special care to be taken of it. This can necessitate that staff receive specific training and instruction in the matter of confidentiality of patient records and the data protection requirements for medical data, this can be include "*an overview of the importance of patient confidentiality*", ICGP/GPIT Data Protection Working Group. (2011).

There have been examples of when sufficient observation of such requirements was not paid, for example,

> "*In the case of Isis Machado mentioned earlier, she was charged and fined under HIPAA for disclosing individually identifiable medical records*"
>
> Johnson, (2009)

It is not possible to speculate if better training would have prevented this instance of a data breach, but what can be commented upon was that under HIPAA there were repercussions for such a breach. In the context of small medical practices, when examining their requirements form an internal perspective, while the relevant legislation may provide the impetuous for protecting the medical data, the medical practice will require its own tools and mechanisms to help ensure staff are not responsible for data breaches.

To this end the ICGP/GPIT Data Protection Working Group, (2011), recommend that practices "*Ensure confidentiality clause is present in staff contracts*". This provides the practice with a tool with which to enforce the requirement upon staff to ensure and maintain the confidentiality of the medical data that the practice is entrusted with.

2.3.4 Requirements for technical and procedural controls to access PHI

In order to maintain the security of the systems and services in small medical practices strong passwords are recommended, (General Practice Information Technology Group, 2008). In addition each user should have their own individual logon credentials that provide them access to the necessary systems and data, and those credentials should not be shared with other staff of the practice.

Locum doctors pose a particular problem. Locums are doctors that cover during another doctor's absence and can be in a practice on a short term and irregular manner. They will require access to the practices systems and medical data to facilitate their treatment of patients and such access is considered to be appropriate, (ICGP/GPIT Data Protection Working Group, 2011). In order for locums to access the practice systems they will need logon details, as with other staff it would be best if they were given their own unique logon credentials. In addition locums should be afforded "*the opportunity to become familiar with practice guidelines for clinicians on use of the IT system*", Department of Health & Royal College of General Practitioners, (2005).

The matter of staff joining and leaving the practice also needs to be handled by small medical practices to ensure their ability to control access to the medical data that they are charged with protecting. Recommendations include, "*A user registration and*

removal policy should be put in place", General Practice Information Technology Group, (2008). This would entail procedures to remove the access to the practice systems from a user who has left the practice, by changing the password for their account or removing their account for example. Also, when a new member of staff joins they need to be facilitated with access to the systems they require but the level of access they require should be closely controlled so that they receive only what they need to do to perform their role.

2.3.5 Physical file protections

Small Medical Practices will still have some amount of paper-based records, referral letters for patients for example. This matter poses two problems for the small medical practices to solve.

Firstly while the paper records are being retained and stored it is necessary to do so in a secure manner, for example there should be no access for members of the public the room where the files are stored and the filing cabinet that they are stored in should be kept locked when not in use, (General Practice Information Technology Group, 2008).

Secondly, when the need to retain the paper records has passed they should be disposed of in such a way that retains the confidentiality of the information contained within them. One solution to that is to shred them and a cross cut shredder is recommended in some guides, e.g. (National General Practitioner Information Technology Group, 2009).

2.3.6 Additional policies required

There is no specific timeframe specified for the retention of medical data by small medical practices, (ICGP/GPIT Data Protection Working Group, 2011), but the same source also lists some related guidelines. It would be good practice for practices to consider the amount of time that they retain their medical data for. If they decide not to implement a specific timeframe after which the data would be expunged then they should continue their efforts to protect the data and ensuring its confidentiality. If the decision is taken to expunge data after a period of time, robust practices would be

required for the destruction of both physical paper based records and any electronic records that are to be destroyed.

Under the Data Protection Act, (1988), data subjects have the right to access the data that is stored on them. This means that should a data subject of a practice request a copy of the data that the medical practice retains on them the practice is obliged to facilitate the request, with the exception of some circumstance's, such as disclosure of the records posing a risk to the physical or mental well being of the data subject, for matters of national security.

If such a request is received there is an onus on the medical practice to maintain the confidentiality of the data subject, e.g. the data should only be provided to the patient in question, it should not be provided to another party unless there are exceptional circumstances for such, to a parent or guardian for example. Such matters can be complex, thus it would be beneficial if the practice were to formalise the process for these requests, while keeping in mind that each request will be different and will have to be treated on its own merits.

2.4 Technical responsibilities and guidance

Neither the Data Protection Act, 1988, nor the Data Protection (Amendment), 2003 mention the word's technical, technology or computer in their text. Considering that it was the information age we live in and that much of the data that is to be protected will be stored in an electronic, digital form this is surprising. How are organisations and companies working with such important personal data expected to protect the data with which they are entrusted when it is stored digitally?

Here the EU Directive 95/46 (Data Protection) goes further with Article 17, which outlines measures for the security of processing private data.

> "*Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the*

transmission of data over a network, and against all other unlawful forms of processing.
Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected"

EU Directive 95/46 (Data Protection)

There are no specific recommendations or requirements in regard the state of the art of technology that should be used to protect the data in question. This situation is echoed in Room, (2008), which explains that specific guidance on such matters is not given by the United Kingdoms Data Protection Act of 1998 and the only technology identified by the act is encryption.

Yet, perhaps this vague statement of the technical guidelines and the flexibility it lends is more appropriate given the nature of technological change, in particular to security related mechanisms such as encryption. For example the Data Protection Act, 1988, could had specified the use of DES[3] standard encryption for the protection of health information, which would have been reasonable since DES was the standard for such protection at the time. The Act would have needed to be revised after the successful brute force breaking of the DES standard in Verser, (1997).

Interpretation of "*appropriate technical measures*" however may be difficult, particularly when this task has to be performed by a person who does not have the relevant technical expertise to understand the state of the art within the field. This is a problem area for small medical practices, who typically will not have a member of staff with such expertise.

When you contrast the EU Directive 95/46 (Data Protection) with article 3 of the EU Directive 1999/5/(Radio equipment and telecommunications terminal equipment),

[3] Data Encryption Standard (DES), http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf, last accessed 28th of March 2011.

which clearly outlines some absolute minimum requirements of the technologies governed, a clear difference is visible.

It must be noted that the EU Directive 1999/5/(Radio equipment and telecommunications terminal equipment) is a far more technically orientated document and deals with a subject matter that is specifically a technical one. This differs from EU Directive 95/46 (Data Protection), a more abstract and procedural based document, the what to achieve of the EU Directive 95/46 (Data Protection), in contrast to the how to achieve it of the EU Directive 1999/5/(Radio equipment and telecommunications terminal equipment). Yet the aim is still the same, the safe guard of community citizens rights, either that of privacy or of economic prosperity, which was the main factor behind the EU Directive 1999/5/(Radio equipment and telecommunications terminal equipment). Further, surely every citizens right to privacy is at least equal to that of their right to economic prosperity and hence at least the community should provide a similar amount of guidance on how that right could be protected?

2.5 Difficulties and requirements originating from data protection legislation

To take an extreme example, an event organiser could be legitimately in possession of information on the dietary requirements of guests attending the event. It is possible that such dietary requirements indicate health information on an individual if such a person is identifiable from such information and information in regards allergies or other nutritional requirements are included. Within the strict wording of the directive such a person may be contravention of the directive if that person is not a health care professional.

Further, it demonstrates that another person, unrelated to the running of the event therefore should not have access to such information without the specific consent of the data subject's in question if the Data Protection Directive is to be taken to the extreme.

This highlights the very difficult position that medical practices are in when personal data is retained, the information they will store is much more sensitive and plentiful.

2.5.1 Requirement for practices to register with the Data Protection Commissioner

Article 6 of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (European Treaty Series, No. 108) stipulates that health data may not be processed unless appropriate domestic law provides safeguards for such. Irish law requires that data controllers that process health related personal data register with the Data Protection Commissioner. These include medical practices:

> "*The following categories of data controller are required to register with the Data Protection Commissioner if they hold or process personal data on computer… Health professionals processing personal data related to mental or physical health.*"
>
> *The Data Protection Commissioner. (2011). REGISTRATION CLASSIFICATION & GUIDANCE NOTES FOR APPLICATION*

Thus, small medical practices are required to register with the Data Protection Commissioner unless "*where such data is processed within the terms of a code of practice approved by each House of the Oireachtas under section 13 of the Data Protection Act 1988*".

2.6 Applying the data protection governance environment to the surveyed small medical practices

This is obviously a complex and broad area with a considerable amount written about it and it is necessary to be able to better understand these matters to examine the implications they will have on the area of small medical practices, which is under investigation. Further, the legislative and governance framework that applies to such area's are not the natural territory for the administrative and medical staff that work in small medical practices nor is it the natural territory for the IT staff who operate there.

This project intends to assess the level of data protection and computer security in small medical practices. This will be done by conducting interviews with key stakeholders in those practices.

This leads to the necessity to try and simplify the complex area so that such staff and researchers can both more easily understand the state of processes and procedures in place in medical practices in relation to data protection, while still maintaining the goals and requirements set out in the regulatory framework. Method of modelling or examining the state of data protection in medical practices would be useful for this purpose.

2.6.1 Data protection checklist for small medical practices

To this end a short checklist has been created to help model and understand the problem domain of data protection in small medical practices. This checklist should not be considered a fool-proof way to guarantee the data protection of medical data in such practices; such an item is beyond the limited scope of this project. It instead intends to provide a mechanism to base the interview section of the project on to help understand the state of data protection in the surveyed practices.

1. Register with the Data Protection Commissioner as a data processor of health data.

2. Define an information management policy for who needs access to health information and how that access is governed. Consider whether administrative staff should be able to access patient information to the same extent that medical staff can, and if they do require such access to what extent do they need to access it.

3. Ensure that access to computer equipment password protected and that screens are locked when staff are not using their computers. Ensure that users do no share usernames and passwords.

4. Implement a strong password strength policy and a password change policy.

5. Have a procedure in place for when locum doctors need access to your systems and record when such access is granted.

6. Have a procedure for when new staff joins to set them up with access to the health information. Also have a procedure in place for when staff leave the practice.

7. Appoint a designated person responsible for security and for periodic review of the measures and practices in place. Establish a procedure for how often such reviews should take place.

8. In respect of physical files:
   Have a procedure for the secure destruction of sensitive paper records, e.g. use a shredder.
   Control and restrict physical access to paper records with the use of locked filing cabinets or rooms

9. Ensure staff members are trained in security and data protection matters and made aware of their responsibilities.

10. Ensure all persons in the practice (not already covered by a professional confidentiality code) have signed a confidentiality agreement that explicitly makes clear their duties in relation to personal health information and the consequences of breaching that duty.

11. Implement a data retention policy, i.e. how long to maintain records on patients for. This will require a defined policy on retention periods for all items of personal data kept in addition to management, clerical and computer procedures in place to implement such a policy.

12. Implement a data subject access request process. This is when a patient or another person or body requests access to patient records.

2.7 Conclusion

This chapter has introduced and broached the legal frameworks that exist in relation to data protection for small medical practices, while it is not possible to cover the entire gambit of the regulatory and legislative framework, it is hoped an adequate representation of the of the area of data protection in the context the medical practices has been achieved, with particular focus on some important points that effect the practices, particularly from the perspective of the confidentiality of the medical data that they protect.

From this a checklist has been created that will help both the practices understand the state of data protection from the confidentiality view point in their environment and this checklist will also help drive the data protection portion of the primary research for this project.

3 COMPUTER SECURITY FOR SMALL MEDICAL PRACTICES

3.1 Introduction

The legal imperative to protect the Personal Health Information, (PHI), that applies to small medical practices has been detailed in the previous chapter. What remains to be done is to examine the state of the art for computer security in relation to small medical practices. The nature of the systems utilised by small medical practices in Ireland is important, much of the literature applies to larger institutions and organisations, while such literature is still valid and important, a special focus on what applies to small medical practices is also required.

3.2 Computer Security Overview

3.2.1 Computer Security Objectives

The common goals of computer security are commonly regarded to be confidentiality, integrity and availability, (Aceituno, 2005). Where confidentiality is regarded as the intention that certain information is only available to certain authorised users and processes, integrity is the ensuring that the information being stored and processed is accurate and truly reflects the state of the data in question and availability ensures that the data is available to the users and processes who have a legitimate requirement to access it when they require such access.

In (Aceituno, 2005), the use of a set of security measures to define security is debunked when comparing the use of a bicycle lock to secure a bike in the English countryside as opposed to Mogadishu. This is an important concept to understand from the perspective of computer security. Measures can be taken to protect any system or item of worth, but those measures are relative to the worth of the asset to be protected and the security environment in which it resides.

3.2.2 The importance of the protection of medical data in small medical practices

Taking the protection of PHI in small medical practices, the General Practice Information Technology Group, (2008), when discussing the loss of existing information technology assets in General Practice surgeries the authors, who are themselves General Practitioners, state "*If you have no data, you have no business*". Also the potential for the loss of trust from patients of their GP if the confidentiality of that data is compromised could have negative consequences for the GP's business as well as the patient's state of mind.

The assumption is that the medical data that small medical practice retains is an asset, which needs to be protected, and the measures used to protect that data must be consistent with the risk or potential risk that the data is at.

3.2.3 Approaches to providing security

Tulu & Chatterjee, (2003), present a general security model for Trusted Third Party Services, (TTP). A TTP is a body that facilities communication between two systems or parties who both trust the third party which allows the originating and receiving parties in the communication to trust each other. The security model emphasises application security on the part of the communicating parties and communication security between them and the TTP, it is similar in some aspects to the Bell – LaPadula model, (Bell & LaPadula, 1973), whereby moving between secure states it is possible to retain the security of a system and the confidentiality within it. The paradigm does not have to apply only to TTP based communication of a global scale where diverse systems from multiple organisations are communicating with each other. The same model's, moving between secure states, achieved via utilisation of application security at the endpoints and communication security to facilitate the data transfer can be applied within a small network or even within single system.

If a small medical practice is to use computer systems that communicate with each other then this approach can help to protect the confidentiality within those systems. It can also provide scale, differing levels and layers of protections can be built into the overall security model whereby application and communication security are employed

to transition between secure states within the same or differing systems. Tulu & Chatterjee, (2003), then move on to apply the security model to the security rule of HIPAA, a hybrid framework for securing HIPAA protected data is developed that addresses the technical and organisation issues faced with HIPAA compliance. An eight-stage process is outlined to make an organisation HIPAA complaint should it wish to become so. While HIPAA does not apply within the context of small medical practices in Ireland, a framework that is intended to achieve such compliance is relevant as it may have commonality with requirements under Irish data protection legislation. However in the case of Tulu & Chatterjee's framework, while it is a useful tool it is somewhat abstracted and conceptualised for application by small medical practices in Ireland. The detail of what exactly needs to be done and how to approach it to maintain the confidentiality, integrity and availability of medical data is lacking.

3.2.4 Computer Security Models

In order to understand how to achieve security for an organisation and what measures need to be taken to protect the information and the systems that store and process that information for the organisation an overall view of how to view and model the concepts behind the specifics of applying security will be beneficial to understanding the problem domain.

A security Architecture blueprint, (Peterson, 2006), which moves from stakeholder goals to provide assurance by streaming security services into differing self supporting streams that help to provide a layered, in-depth defence for information assets. It defines security architecture as:

> "*Security architecture: unifying framework and reusable services that implement policy, standards, and risk management decisions. The security architecture is a strategic framework that allows the development and operations staff to align efforts, in addition the security architecture can drive platform improvements which are not possible to make at a project level*"
>
> Peterson, (2006)

It also outlines processes such as software development lifecycles and vulnerability management that are key to assurance. Each process and defence measure is categorised into a separate but interdependent layer that will help to achieve security. To provide a defence in depth all such measures are self supporting and exist in a holistic environment where the total of the parts working together is greater than the sum of the individual protections.

In Stoneburner, (2001), the security objectives of availability, integrity, confidentiality and accountability are detailed and the notion that once all four of those have been met assurance will be achieved. A security services model, which takes the approach of using key foundations of security such as identification and system protections, i.e. least privilege and process separation to provide a mechanism whereby the user of a system has their access to the resources controlled via authentication and authorisation, among other methods, in a secure manner. The model classifies services according to their primary role, Support – generic, Prevent – preventing a breach and Recover – detection and recovery from breach.

Of particular interest are the components of the model, while no specifics are mentioned, resources such as operating system security services are harnessed and underlie all distributed services. System security can be no stronger than the underlying operating system and the other systems and services around it are intertwined from a security point. For an example that could impact a small medical practice, a Health Information System, (HIS), could be linked to an email client via copying and pasting medical records from the HIS into an email that a user sends to themselves. The medical record could then be compromised by malware on a PC that opens the email. This illustrates the inter dependent nature of security and the necessity for security domains:

> "*A domain is a set of active entities (person, process, or device), their data objects, and a common security policy*"
>
> Stoneburner, (2001),

Essentially establishing security domains is like building fences between data and process flows to impose restrictions between them. This will help to provide assurance, which is a key theme that the important information is not at risk. The paper also distinguishes between the following,

- Vulnerability's, which are weaknesses in system security that could be exploited and would be a violation of the system's security policy
- Threat source's, either accidentally or intentionally triggering the vulnerability
- Threat's, potential for the 'threat source' to be exploited
- Risk – net business impact "*probability of occurrence combined with impact*"

The overall context of the risk management process is elaborated on. A typical example of how this might progress could be a vulnerability in the operating system of server that a small medical practice employs. If the threat source is mitigated by only allowing trusted users an computers connect to the server via the local network and implementing a firewall that prevents access to the server from the internet then the threat is reduced as the potential of the threat source to be exploited is limited. Thus in the balance the matter the risk of the vulnerability to the medical practice is reduced.

3.2.5 Enterprise Information Security Architecture

Enterprise Architecture is a method by which an organisations Information Technology assets and procedures are aligned with the core mission and operational characteristics of the business, National Institute of Health Enterprise Architecture, (2008). Changes from the security perspective have been made to this approach, "*Information security was recently incorporated into EA as enterprise information security architecture (EISA)*", Oda et al, (2009), which profiles Enterprise Security Information Architectures, lists them and provides their chronology.

The four concepts of business, information, technology and security architectures, are introduced and importance and use of abstraction is explained, "*The common levels of abstraction used in the three frameworks mentioned earlier are conceptual, logical, and implementation level*". This provides a hierarchical conceptual model by which to understand EISA and how to apply it. In addition EISA frameworks such as the SABSA method are explained. The SABSA method is is a methodology for EISA, that aims to ensure that security services for a business are designed, delivered and

supported as an integral part of the businesses governance and operations. Some case studies are also presented.

> "*The SABSA method is used in organizations such as the Centre for Medicare Services (a.k.a. Health Care Financing Administration), which is a governing party of Health Insurance Portability and Accountability Act (HIPAA)"*
>
> Oda et al, (2009)

Another EISA example is ISO IEC 27799 2005 – Information technology — Security techniques — Code of practice for information security management. This ISO standard outlines why information security is needed and what needs to be done to achieve it from a high level. It is a broad document that encompasses many of the area's that need to be worked on to achieve information technology security. For example it includes human resource security measures like the use of contracts to protect and organisations information. From the perspective of small medical practices this is important for administrative staff as outlined in the previous chapter. Administrative staff will not be covered by professional standards and practices and require an additional mechanism to ensure their compliance with information security practices.

The ISO also mandates such matters ranging from physical and environmental security management like restricting physical access to information technology assets to the establishment of incident response procedures.

From the perspective of small medical practices the standard outlines how to establish security requirements, assess the risk to the organisation including any legal frameworks when taking into consideration the principles and objectives that the organisation has developed for itself. Risk Assessment will then help guide the business and aid in selecting the necessary risk controls. Risk assessment must consist of both risk analysis, the process of discovery and classification of risk, and risk evaluation, the estimation of the significance of the risk. There is an implied trade-off to ne made, the ISO states that there is a need to "*balance the investment in*

implementation and operation of controls against the harm likely to result from security failures", (ISO IEC 27799 2005).

From the point of view of a small medical practice this is important, there are risks inherent in storing and maintaining electronic records for patients but perspective is required, this is similar to what was argued in the previous chapter in relation to data protection for medical data where it was stated that, "*measures shall ensure a level of security appropriate to the risks*", EU Directive 95/46 (Data Protection). There is a further caveat to this though, such measures and practices are not 100% guaranteed to ensure the protection of such data and,

> "*It should be kept in mind that no set of controls can achieve complete security, and that additional management action should be implemented to monitor, evaluate, and improve the efficiency and effectiveness of security controls to support the organization's aims*"
>
> ISO IEC 27799 2005

This is high-level material without anything practical, it is what to do as opposed to how to do it. For example, in section 10.9 of ISO IEC 27799 2005, protection of electronic commerce assets is mandated but no particulars as to how to do that are available, e.g. there is no mention of the requirement to apply security patches to a MySQL database if that is where the electronic commerce data is to be stored or using encryption at the application layer when electronic commerce services communicate with clients.

This is similar to the other EA security frameworks reviewed as they are are high level approaches for large organisations with multiple layers of management, what is needed for small medical practices is different, they require something more focussed and applied that is easy to understand and implement to start with. For example the NSA has recommended that for home networks, are similar to the small networks that small medical practices may use, install Windows 7 or Vista instead of Windows XP, (National Security Agency, 2011).

3.3 Security in relation to Health Information Systems

3.3.1 Definitions of health data related systems

Small medical practice may use some class of Health Information System, (HIS), or Electronic Health Record, (EHR), system's to maintain and manage their patient records. An EHR system is a record for patient medical histories maintained over time, HIMMS, (Unknown). While a HIS is different in that it may not necessarily focus solely on patient records like EHR systems do and the HIS can include other line of business functions such as billing or appointment scheduling. A HIS and can be defined as:

> "*A system that provides information management features that hospitals need for daily business Features Pt tracking, billing and administrative programs; may include clinical features*"
>
> McGraw-Hill Concise Dictionary of Modern Medicine, (2002)

For the purposes of this project there will be no distinction made between a HIS or a EHR system, they are both being regarded as containing the same sensitive medical data that must be protected as per data protection legislation.

These systems are obviously major stores of PHI and medical data and as such they warrant a special investigation as to the state of the art for protecting them.

3.3.2 Security models for HIS and EHR systems

In Blobel and Roger-France, (2001), object orientated techniques, including the use of UML Use Case diagrams, were developed to create a layered security model for analysis of secure health information systems. This is an interesting approach as it introduces common object orientated software design principles and practices to the area of data protection for small medical practices and holds the potential to enable IT professionals and non IT staff working in the area to better understand the area of data protection.

A "*Layered security model based on a concepts–services–mechanisms–algorithms view*" is presented. It defines the security domain as having shared security policies for the systems in question and different levels of granularity are used. Again, as per Tulu & Chatterjee, (2003), differentiation between communication security, commonly identification and authorisation, and application security, typically authorisation and access control, is drawn, but the security elements that make up each domain, such as DES, MD5, encryption, share commonality between the two and are each repeated in the communication and application security domains.

This shows the mutual nature of such protection mechanisms, their use can be repeated across varying domains and there is a limited set of security mechanisms, such as encryption provided by the AES algorithm, transport security provided by certificate usage such as is employed in TLS and SSL systems. In addition, the repeat of their use provides defence in depth and a layered security model through their repeated usage. Blobel and Roger-France, (2001), go on to list the security services provided by protocols on different ISO-OSI model layers.

3.3.3 Non technical processes required in relation to security of Health Information

Kenisberg, et al, (2004), deal with Electronic protected health information (ePHI), and stipulate that there should be an institutional plan which acts as a reference, assigning roles and responsibilities as well as authority where necessary to ensure the protection of the electronic health information. They state that such a,

> "*at minimum, should explain the method of organization or governance, reporting mechanism, and training component*"
>
> Kenisberg, et al, (2004),

In order to ensure HIPAA compliance, it is necessary to have an organisational process as opposed to static implementation of the requirements as interconnected elements require governance. This can have an impact on small medical practices as there may be a number of interconnected practices and processes that are important to manage to

ensure the security of the medical data that the practice maintains. For example, assigning user roles to administrative staff that limit them to only the level of access they require to perform their job, coupled with a policy that prevents the sharing of usernames and passwords to prevent a "side door" of access to a system that such staff should not have access or a particular form of access to. It is necessary to look on such matters from a "big picture" viewpoint, instead of looking at the individual matters at hand, there instead needs to be an overall strategy and awareness of the need for protection of the sensitive medical data.

In order to achieve this ePHI must first be uncovered and the repositories in which it resides identified. For example does such data exist in cross organisation applications such as a HIS or EHR, or does it exist in single files on workstations? If time is pressing a number of starting questions are listed to determine the level of what needs to be done to achieve HIPAA compliance.

> *What assets need protection?*
> *What vulnerabilities exist in the environment?*
> *What is an acceptable risk level?*
> *What controls are necessary to ensure adequate and appropriate (specifically, reasonable) security?*
> *What sort of regular schedule should be created for testing, auditing, and documenting?*
> *Is the incident management procedure sufficient?*
> *What does protection failure mean?*
> *How much protection can the institution afford?*
>
> Kenisberg, et al, (2004),

There are a number of area's that could represent particular problems to the area of data protection in small medical practices. If for example PHI were to be transferred across the Internet there would be requirements for particular security technologies to be used to help protect such information, for example RADIUS, IPSec and or SSL VPN services. In Gritzalis et al, (2005), a wide ranging series of technical guidelines for data protection in medical environments is presented. The depth of such protections

varies from user specific measures such as limiting the use of use of email distribution lists, to more technical matters like support for the mentioned security measures of RADIUS and VPN by internet service providers and the use of contractual obligations to manage such providers.

The application to small medical practices of what is discussed in Gritzalis et al, (2005), is important and it also displays the disparity of protection measures necessary on their part. Simple matters such as the use of the wrong email distribution list could put medical data at risk. All the way up to the N tier architectures being secured, i.e. the data base server and web server for a distributed HIS being secured. The wide range of necessary protections necessary for small medical practices can not be over stated, once medical data is in a digital format there are far more avenues for it to escape from the intended state it was designed to be in.

3.3.4 Understanding the security available in HIS and EHR systems

HIS systems are software that require a particular examination of their security attributes due to the nature of the data they process, in Blobel et al, (1999), modelling of users security needs is undertaken using UML again and the different types of security related use cases are mapped out, such as the access control and user authentication use cases. These are components of any system that requires granulated access levels to the data contained in the system. From this an abstract security model for the design and development of systems that manage and store health records which has system security requirements identified and designed into it from the start. This will be of particular use for software developers and possibly systems integrationists.

While understanding the mechanisms used to secure applications and systems is important, it will not always be possible to gain the access to the source code necessary to be able to delve into the detail required to determine if such security practices have been implemented. Blobel, (2004), discusses authorisation and access control for electronic health record systems, particularly for integration between differing organisations EHR and HIS systems. While such a scenario of integrated, cross organisation systems is unlikely to effect small medical practices that exist in a state more in akin to a sole trader and do not have such inter-dependences and links with

other organisations so that their HIS systems are directly linked to another's, the methods used to understand policy definition, agreements, authorisation and access control between such systems can be harnessed for the use of small medical practices to better understand the protections built in to their HIS systems. To such an end, Blobel, (2004), mentions the Health Informatics standards that Blobel has contributed to, ISO TC 215 Health Informatics, which deals with matters of interoperability between health informatics systems.

3.3.5 Standards available for securing health information systems

ISO TC 215 was not the only such standard discussed in Blobel, (2004), CEN EN 13606 and HL 7 were also mentioned and there are other similar efforts that are not focussed entirely on the security of health information systems that merit some review.

Two of the main organizations that administer standards related to HIS and EHR systems include Health Level 7, (HL7) and Comite Europeen de Normalization – Technical Committee (CEN TC), as per (The MITRE Corporation, 2006). Much of the work in regards the formulation of standards for interoperability of health information systems is underway, particularly in Europe.

> "*The main focus of EHR communications standardisation is presently occurring at a European level, through the Committee for European Normalisation (CEN). The major constructs of the CEN 13606 model are outlined. Complementary activity is taking place in ISO and in HL7*"
>
> Kalra, (2006)

The HL 7 Security initiative state that:

> "*This group supports the HL7 mission to create and promote its standards by publishing standards for trustworthy communication among all applications and services in HL7s scope. The Security TC also will lead the convergence and harmonization of standards for identity and access management among healthcare standards development organizations*"

Health Level Seven International, (2005)

This is supported by CEN 13606 - Health informatics, where part 4 of the European standard deals with security and defines measures to support access control, consent and auditability of EHR communications, (Kalra, 2006).

Further ISO 27799:2008 specifies detailed guidelines and best practises to maintain the confidentiality, integrity and availability of personal health information, (ISO 27799:2008). The standard is very detailed when outlining what needs to be done to help ensure the information security management for health data is adhered to, for example it mandates:

> "*Organizations that process personal health information should take sensible steps to ensure that the public are only as close to IT equipment (servers, storage devices, terminals and displays) as physical constraints and clinical processes demand*"
>
> ISO 27799:2008

However, while this level of detail is achieved for such matters it still does not elaborate on the specific technical tasks that are required to ensure that the health information is secured.

3.3.6 Application development standards for non Health Information specific systems

The standards discussed so far can be useful in identifying systems and software that meet the stringent requirements necessary to ensure that the health information that small medical practices store and process is adequately protected. Yet, if a system does not have certification from one of those standards organisations, that does not necessarily mean that the system in insecure. There are other standards in relation to the development of software in a secure manner that can be used to determine if it has been developed securely, some of these standards will be discussed here.

The OWASP Guide Project's, (OWASP Guide Project, 2011), intention is to help developers of websites and web applications develop such applications in a secure manner. They state "*secure applications cost about the same to develop as insecure applications, but are far more cost effective in the long run*". If this is true it is a strong argument for such development methodologies, particularly if a small medical practice were to be interested in the implementation of such a system, say for example they wished to sue a system that could display available appointment times online. Such a system would need to integrate with their existing appointment management system and if access to PHI were possible or even potentially possible OWASP implementation standards would help allay any fears they may have about exposing the PHI to an increased threat.

In addition, if a HIS or EHR system that the small medical practice used was a web application, such a development methodology could be used in the construction of the web application, further security mechanisms would be recommended at that stage, such as ensuring there were no direct access between the internet and the web application.

The Microsoft Security Development Lifecycle Process, (Microsoft, Unknown), includes foundation concepts such as secure design by reducing the attack surface of the application, the principle of least privilege and defence in depth. It also mandates practices such as Fuzz testing and security reviews. The development lifecycle lays out a step-by-step guide to writing and developing secure applications and as it emanates from the Microsoft environment is of particular use to any applications that are developed for use with Microsoft systems.

For small medical practices this is important if they are to purchase health information systems that will be run on a Microsoft Server Operating System and accessed by Microsoft Client Operating Systems. Software that is developed to the Microsoft Security Development Lifecycle Process will provide a level of assurance for the protection of that software.

The standards of application development laid out above will have common secure coding techniques throughout them and there are some things when developing software that can be done to increase the security of that software, such as validating input, avoiding buffer over flows and checking code manually as opposed to with an integrated development environment alone as well as with automated tools for security flaws, (IT Security Office, Trinity College Dublin, 2005).

The necessity for validating input was highlighted in (McKenzie, 2011), when examination of an open source social networking web application developed in Ruby would allow any authenticated user the authorization to interact with any other users pictures because the object ID that was used for the pictures was not a private object and could trivially be guessed by another user. There was no validation of the input that a user could enter to ensure that they were authenticated for the action they had requested.

The outlined security weaknesses were found because the project was an open source one and in some ways this example is an argument for the security of open source systems as they allow peer review of their code. This option may not be open to small medical practices as they are unlikely to have direct access to the code of a health information system that they may purchase off the shelf from a vendor. But asking the question about the security reviews that took place during the development of the application can aide in determining if the health application had such security matters considered when it was being developed, assuming of course that any answer that was received was truthful.

3.3.7 Limitation and overview of standards

The use such security standards are to be put to within small medical practices for the purposes of this project must be understood. It is not assumed for the security model that is being developed for this project that if a health application in use in a small medical practice does or does not have certification from one of the mentioned standards that it is guaranteed to be secure on unsecure as the case maybe. The intended use of these standards is as a guide to the security of a health application, such standards are not he last word in security.

Essentially the standards discussed in this section deal with what could be done with the personal health data being stored and processed via the health information systems software and applications employed by a small medical practice. The standards provide guidance on how to seek assurance that these applications interact with the data in a secure manner.

There is more to the eco system of systems a small medical practice may employ than just the HIS application that processes the PHI directly, e.g. the network that the data passes over or the servers that the HIS run on. There are also recently developed security incidents and problems that may influence data protection and security matters for health information.

3.4 Recent Security Problems

There had been a large number of well-publicised security incidents at the time of the writing of this dissertation. These are important to note because they reflect some common problems with securing any kind of information system but also because they may influence stake holders in health information systems, such as General Practitioners and patients as to the level of security that is needed to protect personal health information.

3.4.1 Examples of recent security problems

These include attacks that exposed the information of millions of users of the Sony online gaming network, (Goodin, 2011 - A), because the web servers that the information was accessible through were running out of date versions that had well documented security vulnerabilities, in addition to the fact that there was no firewall running between the servers and the Internet.

Attackers were able to access the account information for 200,000 Citigroup customers, (Goodin, 2011 - B), through a common underlying vulnerability in the company's website that was another example of a lack of validating input:

> "*The technique allowed the hackers to leapfrog from account to account on the Citi website by changing the numbers in the URLs that appeared after customers had entered valid usernames and passwords*"
>
> Goodin, (2011 - B)

An alarming, but thankfully subsequently debunked rumour, (Oates, 2011, A), was circulated on the Internet that the Lulzsec group had gained access to the UK census data. As mentioned the rumour turned out to be without foundation, but possibly the more concerning matter was that such a rumour gained credence at all and was not immediately dismissed as impossible.

Another example of a serious attack that occurred because of a lack of basic security mechanisms was the attack on HBGary Federal, (Bright, 2011), that occurred because a password fro one user was obtained through he use of an SQL injection on the content management systems for the company's website yielded a password that was re-used for other systems. The SQL injection could have been prevented through updating the content management software for the website in question.

Other examples of data breaches include Lockheed Martin suffering a data breach in part because of the compromise of the RSA authentication tokens that they used, (Goodin, 2011 - C) and (North Atlantic Treaty Organisation, 2011), where a website operated on behalf of NATO that ran their online bookstore suffered a breach.

While not an example of an explicit technical failing, (Brook, 2011), details how the University of California at Los Angeles Health Services were fined for employees gaining access to the health records of celebrities without proper cause. Another example of insufficient security of health records related was when the NHS in Britain, (Oates, 2011, B), signed undertakings with the Information Commissioners Office to improve processes in relation to data security of medical information.

3.4.2 Impact of these attacks on securing health information for small medical practices

Thankfully none of the cited examples are examples from small medical practices but that does not mean that small practices are immune to such matters. What is of particular concern is that there are some common threads of concern between many of these examples.

Firstly several of the attacks emanated from the Internet and targeted web servers and web applications that stored and processed the information that was lost. Secondly, a number of the breaches could have been prevented by implementing simple security remediation's, such as updating software or not re-using passwords between systems, they were not that difficult to prevent.

Thus this project will examine more commonplace security mechanisms and guidelines that may be applicable to small medical practices in order to mitigate against the types of attacks discussed by this section. This requires more applied guides and standards for securing common systems and services that may be used in small medical practices than have been discussed to date.

Such guides will have more bearing on the foundation and platform on which the health information data is stored and processed, such as servers that run health information systems and store health data, network devices that communicate health information between end points and client computer operating systems that integrate with the health information systems. These are systems and services that are likely to be used in small medical practices and due to this require some examination.

3.4.3 Further considerations for the protection of personal health information

Thus far we have examined protection of health data when it is being processed and some of the common problems that have publically impacted information technology users of late. There are other considerations to take into account for the security of health data in small medical practices though. For example we also need look at the security of such data when it is stationary within a system and being moved between

systems as well as how it gets into any health data repository and what can access it when it is there.

3.5 Security of ancillary systems that provide a platform for health information systems

There are a number of ancillary systems that could connect to a small medical practices network and interact with the health information stored their, even if the ancillary systems themselves are not the primary repository for the health information. These systems provide the foundation and platform upon which the other specifically health rolled systems reside and because of this require consideration for the security of the network as a whole.

A common client operating system that may be in use in small medical practices is Windows XP. Client computers can connect to the practice network and access shared IT resources such as a health information service, because of this dependency and the fact that it increases the attack surface for the practice network as a whole there is a need to ensure that such client operating systems are secure. Practices such as not allowing users to have administrative privileges and applying security patches quickly after their release are common client security mechanisms, Scarfone et al, (2008, A), details these mechanisms and others, such as security template's, which are text-based files containing configurations for security-relevant system settings that can be applied across a network of client computers to ensure a common baseline security configuration on each.

As client operating systems can be secured, so to can server operating systems and small medical practices may employ a server to facilitate shared information technology resources such as a HIS.

One example of the guides available is the Windows Server 2003 Security Compliance Management Toolkit, (Microsoft, 2009), which provides information about how to harden servers running Windows Server 2003. It is a utility that can be run on a server which "includes updated security guides, pre-defined group policies, the GPOAccelerator tool, and Configuration Packs" Kleef, (2009), to harden the security

posture of the server. There are similar guides available for Unix operating systems, for example, (AusCERT & CERT/CC, 2001), which while it does not provide an automatic way to run the check list it does provide considerable detail on how to secure a Unix based operating system. For example much attention is paid to the necessity to install software patches, both for the operating system software and for any application software running on the server.

Protection of such systems, both Unix and Windows, even if they do not themselves store or process health information and even if they are not intended to be able to access health information is still important. Such ancillary systems may provide trusted services to a small medical practice, such as DNS or directory services, upon which the HIS application relies and trusts. General sever security is discussed in (Scarfone et al, 2008, B), which provides a security policy that can be applied to such servers and is of particular interest from a change management perspective and for security planning and maintenance of ongoing server security over time.

An area that is of importance for ancillary systems and services that can interact with health information systems in a small medical practice is any directory service that is running on the network and providing authentication for users of the HIS. Such a directory service is in a position of trust on the network; the systems that integrate with it have to rely on it to provide secure and reliable authentication services. ISO/TS 21091:2005. Health informatics -- Directory services for security, communications and identification of professionals and patients, deals in particular with these concerns. While this standard is more to do with the design of authentication mechanisms for health information systems than for the assurance of security of a particular network directory service, it still serves to highlight the importance of the matter.

3.6 Security of medical data when it is at rest

Data can be at rest in small medical practices when it is not being processed but is simply being stored. The confidentiality or availability of the data could be at risk if there is no mechanism to ensure its protection, say for example if the storage media that the data is at rest on were mislaid or stolen. If such a case were to happen an effective way to protect the data would be to encrypt it. One effective encryption

standard is the Advanced Encryption Standard, (AES), as per (NIST, 2001), which details the cryptographic algorithm that can be used to protect data by turning it into a cypher text that can only be read with the key that was used to convert it into a cypher.

Small medical practices can store data on storage devices such as hard disks or magnetic tapes. When the storage media is no longer to be used the data on it could still be at risk if the data is not destroyed in a secure manner. Procedures for data destruction are available as per (NSA, 2000), which include mechanisms such as incineration and degaussing to ensure that the confidentially of the persona health information is maintained after the storage media the information used to be stored on is retired.

Another possible scenario that could place data at risk when it is being stored is if it were to be stored in a cloud based storage facility that may place it out of the control of the data controller. ENISA, (2009), details a checklist for cloud computing services that can be used to seek assurance that the cloud based service is not putting the confidentiality, availability or integrity of the data at risk.

3.7 Security of medical data when it is in transition between systems

Medical data and personal health information in small medical practices has the potential move between intern connected systems on a small medical practice frequently. Because of this there is a need to apply protections to the data when it is in transit and the network over which it transits in order to maintain the confidentiality and integrity of the information.

3.7.1 Network perimeter defense and architecture

If a small medical practice uses a network to allow its endpoints to communicate with each other it will most likely have a perimeter that is connected to the network. Also, the internal network needs to be designed and configured in such a way not to put the data that passes over the network at risk. In order to aide the understanding of such matters and assist the systems and network administrators of small medical practices the state of the art in regards network protection will be of use.

A checklist to help when "*evaluating whether a network is adhering to best practices in network security and data confidentiality*", in the form of a security policy is available in Alabady, (2009). The paper details issues such as router weaknesses, including a list of some attack types and common security policy and configuration weaknesses that should be avoided. Firewalls implement a security policy, what traffic is allowed to pass into the network is configured and then only traffic that meets the policy is allowed to pass through the network. This is relevant because many GP offices have a small LAN connected to the Internet and the routers and firewalls that are used need to be properly secured.

This policy is of particular benefit for the setup of small medical practice networks as it details a total of 20 security mechanisms and best practices that may not always be automatically applied to such small networks. Further the policy is mostly vendor agnostic, so it will not be limited to one particular brand of equipment, such as Cisco or Netgear.

In SANS, (2005), suggestions as how to segment a network for security purposes is discussed. A network segment will be defined based on the security level of each segment, including remote users and a chapter of the paper is dedicated to the securing of remote users via VPN, (Virtual Private Networking). Securing how remote users access the network is important for small medical practices as they may allow staff to work from home and those staff will likely connect to the practice network via the internet. In order to facilitate this some kind of security needs to be applied to the mechanism that is used to allow remote users to connect.

Network protection for small medical practices can then be combined with the guidelines for firewalls and firewall policy in Scarfone and Hoffman, (2009). This guide explains the technologies implemented in firewalls, such as packet filtering and network access control and how to utilize them in firewall policy's and network architectures.

3.7.2 Wireless network considerations

Small medical practices may decide to use wireless communication technologies to allow communication within the practice. If they do so and particularly if it will be possible to gain access to any health information systems from the wireless network, they should consider using wireless security protocols to protect the communication on the wireless network.

The Remote Authentication Dial In User Service (RADIUS), as detailed in (Rigney, 2000), is a networking protocol that manages authentication, authorization and accounting for computers that connect to networks, including wireless networks. For wireless networks used by small medical practices RADIUS can be used to control the users who are permitted access to the wireless network and what network resources they may use while connected.

In order to protect the data that passes over the wireless network the 802.1X Wireless Standard, (IEEE, 2004), uses the EAPOL protocol to enable encryption between segments of the local network, usually between the wireless access point and the wireless enabled device that is connecting to the network. in the case of small medical practices this would help to maintain the confidentiality of the data transiting the wireless network since the data would be encrypted.

3.8 Conclusion

This chapter the state of the art for computer security of health information related systems and services were discussed. A particular emphasis was placed on security from the perspective of small medical practices because the environment in which small medical practices operate is different from that of larger organisations such as hospitals or similar.

Much of what has been written about securing health information systems pertains to large systems that communicate across networks with other complex systems. These are complex scenarios, but small medical practices operate different systems in different environments. They are more likely to have s small local network with a small number of desktop workstations connected to it, with possibly a central file

server that have access to email and other standard productivity systems. If they use a health information system it is likely to be a small localised one that does not share data outside of the network to which it is connected. Much of what pertains to the cross organisation environments envisaged for many health information and electronic health records systems does not apply to the more limited, smaller scale systems that are used in small medical practices.

What is needed to help protect such practices information is understanding of the security mechanisms to protect how data can get into the health information repository and what systems can interact with the process, what can be done to the data once it is in the repository, how it is protected when it is at rest and how it is protected while being transported between systems and the repository.

4 SECURITY MODEL AND DATA PROTECTION FRAMEWORK

4.1 Introduction

The challenge for this project is to offer a holistic security approach for a multifaceted environment where the key asset to secure is the health information that patients entrust to their medical practitioners. This information can reside in a number of locations, e.g. within the electronic health record system that their medical provider use's for patient appointment scheduling and record keeping, to a single file on a USB key, such as a letter to a fellow medical practitioner, that their doctor has taken home to work on later. The important matter here is not the type of method that is used to access or store the health data, although that certainly can have a baring on the protection applied to the health data, the important matter is the health data itself, that is what the patient values and that is what needs to be protected. The question is how to protect the sensitive health data from unauthorised access and this question is where the matter clouds and becomes difficult to manage due to the complex environment that computing can exist in.

This chapter will introduce the technical and procedural security model that is being constructed for this project to better understand how to protect the Personal Health Information, (PHI), that small medical practices retain and process and how that information is currently being protected in the surveyed small medical practices.

This security model will consist of three hierarchical layers, a PHI data classification layer, a systems and services classification and examination layer and a security measures and resources layer. The data classification layer is the top level of the model and it deals with the conceptualised state in which the data exists, e.g. is the data residing within a specific health information system or is it travelling between two systems. The systems and services classicisation layer corresponds to the system which the PHI data is being processed by or stored in and whether or not that systems primary purpose is to deal with PHI. The security measures and resources are the

actual protections applied to the PHI and corresponding references to ensure a compliant security state.

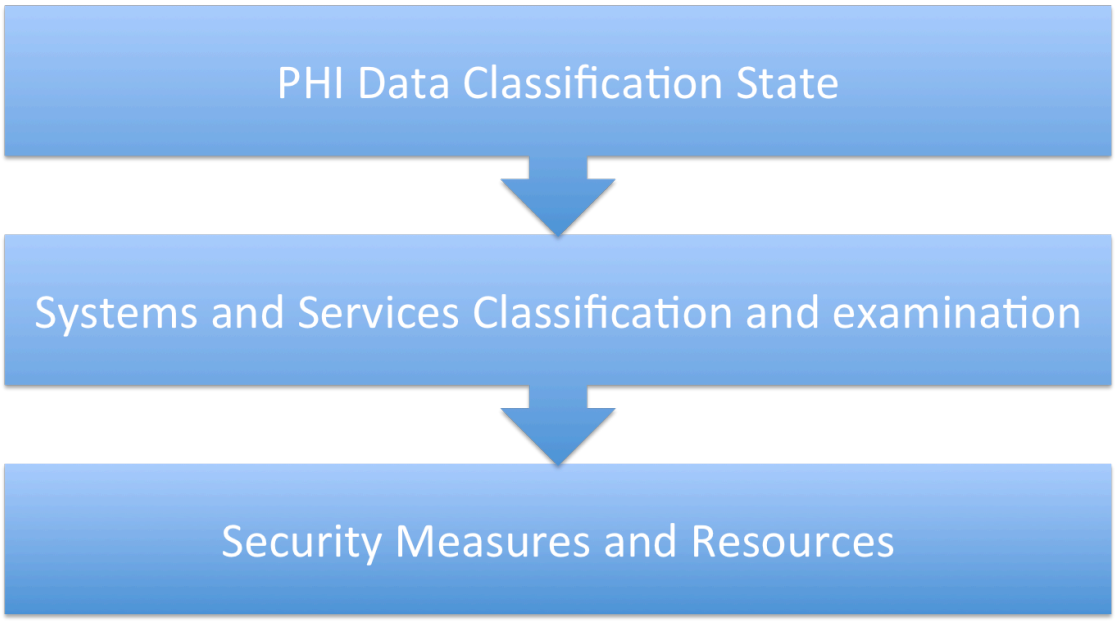


Figure 4.11: Security Model Overview

These layers will be expanded upon throughout this chapter to aid understanding of the security model being constructed. To understand what type of model is needed for this project an understanding of the systems that store and process PHI in small medical practices will be beneficial.

4.2 Typical Small Medical Practice Network

Small medical practice networks will be similar to many other small networks and have corresponding systems. The main differences will be in two areas. Firstly the type of data that is being stored and processed, such PHI can require more rigorous protection than other forms of data, such as timesheets and other office records, which while they will contain personal information, timesheets do not also contain medical data as PHI does. Secondly a small medical practice may employ a Health Information System, (HIS), or Electronic Health Record, (EHR), System, that stores and processes the PHI.

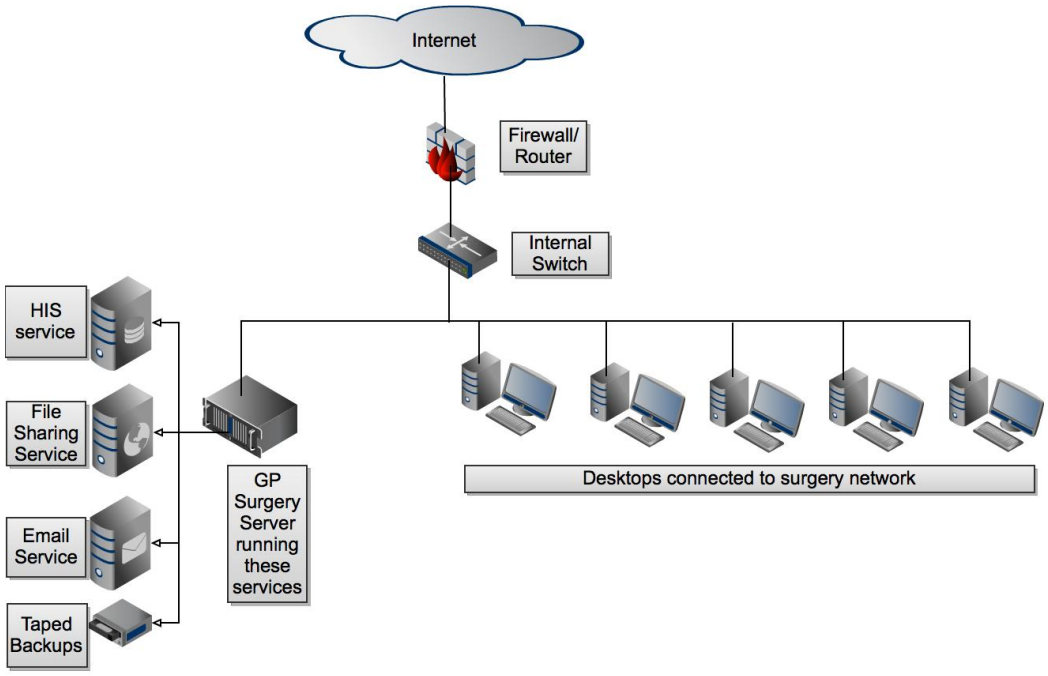


Figure 4.12: Typical Small Medical Practice Network

A typical small medical practice network may be similar to other small office networks, will be connected to the Internet through a router that may also be performing duties as a firewall, (Shafer, M, 2010). The internal network may have a server running a number of services, such as the HIS, email, file sharing. There may also be a taped or other backup solution in place. The internal network will then have a number of desktop or laptop workstations connected to it to allow the staff of the practice use the IT resources. In this instance it is being assumed that the network is a wired network only and that no wireless connections are being used, however the security model will provide controls and security measures for wireless security.

Such a network may have a number of vulnerabilities associated with it, for instance the default configuration including username and password may be left applied to the router that is acting as a firewall, or the server running the shared IT services may not be fully up to date with operating system security patches.

Either of those scenarios has the potential to expose the personal health information stored on the network to the risk of a data breach or other un-authorised access. However, they are not the only possible risk, e.g. if taped backups were being used and

transferred off site but not encrypted, if they are lost the confidentiality of data they contain could be lost, there are multiple risks associated with such a network and a more systematic and comprehensive method to assess the security state of the network and the PHI that it contains is required. One example of when medical data was lost occurred when thieves pilfered backup tapes holding two million medical records, (Fonseca, 2008).

4.3 Approach and perspective of the Security Model

The approach that will be used for this model is from inside the organisation that uses the systems and stores and processes the PHI data. This will be the view from a systems administrator and end users perspective, that is to say the people who will be responsible for implementing, securing and using the systems not the view of a developer or programmer of HIS or EHR software. Nor is it the perspective of a penetration tester or other body testing the systems from an external perspective.

This approach is taken because the intent of this project is to investigate the general level of data protection from within the small medical practices, not from an external stand point. It is not to say that alternate viewpoints are not helpful or valid though, simply that the target audience for this model is an internal audience.

4.4 PHI Data Classification States

For the purposes of this model there are 3 states or categorisations in which PHI can exist within the confines of the systems that small medical practices commonly use.

1. Inside
2. Outside
3. Over

Breaking the model into such segments aides in both understanding the problem domain and in the interpretation and analysis of the problem domain when compared to the model. Instead of having a long list of indicators it is possible to compartmentalise the systems and processes that need to be analysed and deal with

them separately. It will also make the task of analysing the security state of the practice seem more manageable and less daunting.

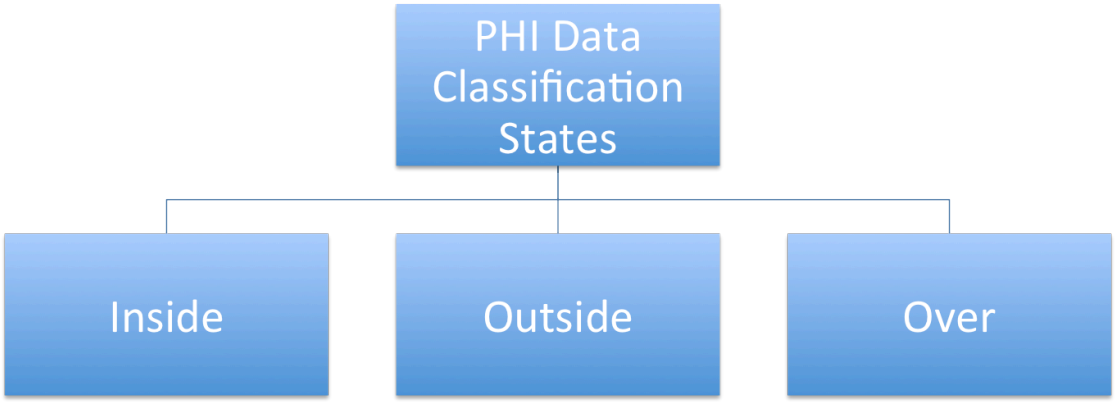


Figure 4.13: PHI Data Classification States, Inside, Outside, Over

4.4.1 Inside

For the purposes of this model this is PHI and medical data when it resides in a system whose purpose and intention is to process and store PHI data. Essentially this will most likely be the Health Information System, (HIS), and or the Electronic Health Records, (EHR), System that the small medical practice uses to manage the health information of its patients.

However the "inside" categorisation may not apply to HIS and HER software systems alone. For example if a practice kept a specific database of medications prescribed to patients outside of their HIS, that would also be categorised as an "inside" state as the purpose of the database is to store data that is specifically medical in nature and is being used for a purpose that is medically related.

The PHI when it is in the state of being "inside" is the primary repository of the sensitive medical and health data that the model being constructed intends to help secure and protect. Thus those systems have a higher level of risk attached to them if

they were to be compromised and require specific attention for the purposes of this model.

From the sample small medical practice network outlined in figure 2 of this chapter the inside data state would apply to the HIS service running in the GP Practice server.

4.4.2 Outside

PHI and medical data is in the "outside" state when it is being stored in or processed by a system that is not specifically intended to store or process personal health information. There are a varying number of such systems including.

1. File Servers that save referral letters sent to patients or other medical practitioners about patients
2. Workstations such as desktops and laptops that have PHI saved locally to them
3. Web Servers or other such systems that are not primary information repositories of PHI but could be used for secondary services such as appointment bookings, in the case of an online booking facility that may be offered
4. Emails if staff in small medical practices have used email to forward personally identifiable health information
5. Another crucial "outside" system would be a directory service that is used for authentication purposes when granting user access privileges to PHI data stores

This is not an exhaustive list of such systems; it is intended just to highlight the potential multitude of them that may exist. The key identifier for these systems is that they can or do store PHI even though they are not the primary information store for such information or that they are in a position of trust and interaction with "inside systems".

It is important to identify such systems as any risk they pose to the security and confidentiality of medical data could easily be over looked. Furthermore the integration they have with the "inside" system could place them in a position of trust, which could be exploited to improperly access medical data. Take for example if there

were a vulnerability on a server that was running the directory service against which the “inside” HIS authenticated users, that could allow access to PHI through a side door, if the security posture of the “inside” system was harder to circumvent than the security posture of a trusted “outside” system, that still puts the medical data at as much risk as if the “inside” systems security posture was poor.

From the example small medical practice network outlined in figure 2 of this chapter the outside data state could apply to the file sharing, email and backup services running on the GP Practice server as well as the workstation computers connected to the network if any of those were to store and process medical data outside of the confines of processing it with the HIS client software they may have installed.

4.4.3 Over

PHI is in the “over” state when it is being transferred between other systems, be they “inside” and or “outside” systems or from one type to the other, i.e. an “inside” system to an “outside” system. That particular case could happen with the example small medical practice network as per figure 2 when the HIS is backed up to tape drive, this is a transfer between an “inside” and an “outside” system.

The other obvious example of an over system is the network that the server and workstation computers are connected to as PHI data will be passing over it. But additional less obvious examples would include PHI being saved on a USB storage device to be transferred from one system to another. The main identifier of “over” systems is that their primary purpose is to transport data, possibly including PHI.

4.4.4 Classification overview

The general categorisations of the systems that are being modelled have been provided. The intention is to provide a holistic approach to assessing the systems and processes that the practices use to store and process PHI and medical data. It is important that individual systems do not receive too much focus. Like any network and group of users who use the network there is interdependency between the elements of the network in addition to the users to ensure protection and security of the data contained within the network. If too much focus is placed on one single system or process, say

protection of the HIS for example, to the detriment of other crucial systems or processes, assigning user access rights perhaps, that can lead to threats that the data contained in the network may be exposed. Hence the necessity for a holistic approach that encompasses all the elements of the network, systems and processes that exist with and around the PHI data that is being protected.

This high-level data classification of "inside, outside and over" is the first step in analysing the security mechanisms in place to help secure and protect that data, a more applied and detailed classification system is required to understand what is needed to be done to secure the PHI data within the "inside, outside and over" model for small medical practices.

4.5 Systems and Services Classification and examination

The systems and services classifications will further be broken down into "Application, Platform and Data".

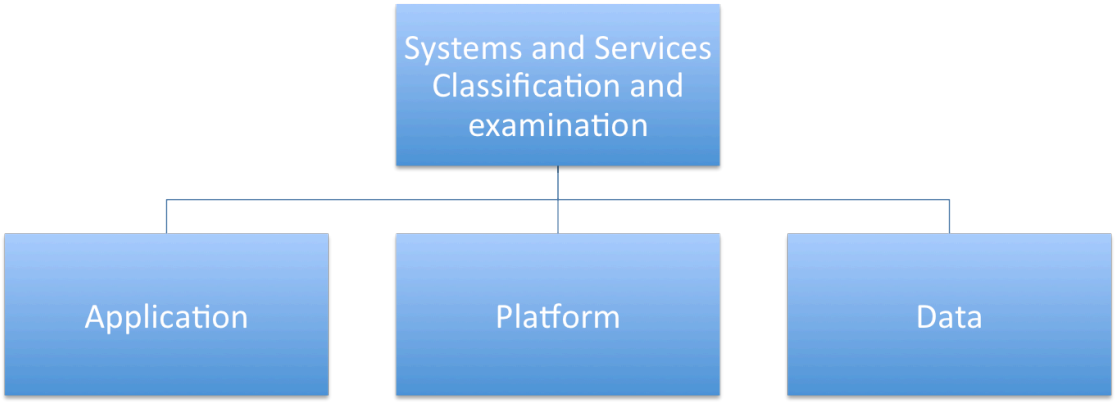


Figure 4.14: Systems and Services Classification and Examination

Within the "inside, outside and over" PHI Data classification states it is important to understand the systems and services within which the PHI data resides. This will be an aide for understanding what is needed to help secure and protect such data for small medical practices, the "application, platform, data" classification will assist in this.

Before going any further however it is necessary to point out that there is much cross-pollination between application, platform and data. For example, to briefly skip ahead for a moment, if reviewing the "platform" segment, i.e. the operating system and configuration of a server that hosts a small medical practices HIS as part of the "inside" component examination, you may also be reviewing at the same time the "platform" segment of the "outside" data classification if the same server that hosts the HIS also hosts the file server that is the "outside" data classification.

The exact details of the "application, platform and data" classifications will be expanded upon further, it is important at this stage to understand the inter-related nature of the systems and classifications. This can lead to a security configuration of one system or service within a PHI data state classification spilling into and covering other PHI data state classifications within the security model. This can lead to duplication within the security model. However because each small medical practice will be unique it is better to have duplication of security checks than to possibly miss a crucial security posture.

This method also lends scalability to the model. While it is small medical practices that are being reviewed the model will also lend itself to the review of larger medical practices as they will have the same class of systems and deal with the same type of PHI information, the size and complexity of the inter related systems is not a limiting factor of this security model. Finally, the perspective taken for the model is that of the PHI data as opposed to the systems. The PHI data can exist in multiple states and it is the data within those states that is to be protected, the protection and security of the systems through which the PHI data of small medical practices store and process that data is only the method with which the phi data is secured.

4.5.1 Application

For the purposes of this part of the model the term application should be considered to cover the main purpose for which the PHI related service is being used. Say for example a server running a Windows Server Operating System was hosting a HIS that stored PHI on the patients for the small medial practices. For the categorisations of this model the application is the HIS system. Another example would be a server that was

hosting a file sharing service to which PHI could or is being stored, in that instance the application categorisation applies to file sharing service.

Aspects of the “application” that need to be examined for security purposes will vary. In almost all instances they will include ensuring that any software patches available for the application are applied and that best practices in the configuration of the application are adhered to. From the development and programming perspective regular third party code reviews and other software security best practices are important. However the problem with such suggestions is the difficulty in ascertaining if they are complied with when the application being developed is being developed and supplied by another who do not have an incentive to inform customers and users of the security features of the product unless it is absolutely necessary to do so.

4.5.2 Platform

The platform classification relates to the systems and services that interact with the “application” and “data” classifications that correspond to the PHI that is being stored and processed in the “inside” state of the systems that a small medical practice may use. For example it would refer to the server operating system security posture where the PHI that is stored and processed resides. It would also cover the “outside” state when referring to the operating system security posture of the client systems that interact with the HIS “application”.

The “platform” classicisation does not refer just to operating systems though. It would also include the anti virus software installed on the “platform” systems and its update setting for example.

There is a broad scope for the “platform” classification within this model, further examples would include directory services configuration and patch management. however this is important because of the large number of diverse systems that can co-exist and interact on a small medical practice network or other network and the trust relationships that may exist between them which could potentially expose the PHI that is been protected to exposure and risk.

4.5.3 Data

For the purposes of this model the “data” classification refers to the actual PHI in whatever format it exists within any of the “inside, outside and over” states of the security model for small medical practices. While the “application” classification may process the PHI data and the data may reside on the “platform” component of the security model, the “data” classification is what the intent is to protect and secure.

For example if the “platform”, (server operating system), or the “application”, (HIS software), were to be compromised but the data was protected, using cryptography for example, then the risk of a data breach of protected health information is much less reduced. Typically cryptography and encryption will be important methods used to protect PHI as well as access controls which restrict the PHI that users and systems that do not need access to the “data” get.

However security through the “data” classification of this security model for small medical practices is not enough on its own though. If the key management solution is compromised through a vulnerability of the “platform” classification within the security model, then the PHI is at as much risk as if there were no “data” classification protections put in place. Thus perspective is required, and a holistic approach is necessary, to provide a multiple layered security model that elps to protect and secure PHI data in small medical practices.

4.6 Security Measure and Resources

The security framework for the systems and services classification and examination layer of the model being designed will mostly be made up of two separate components, configuration and standards.

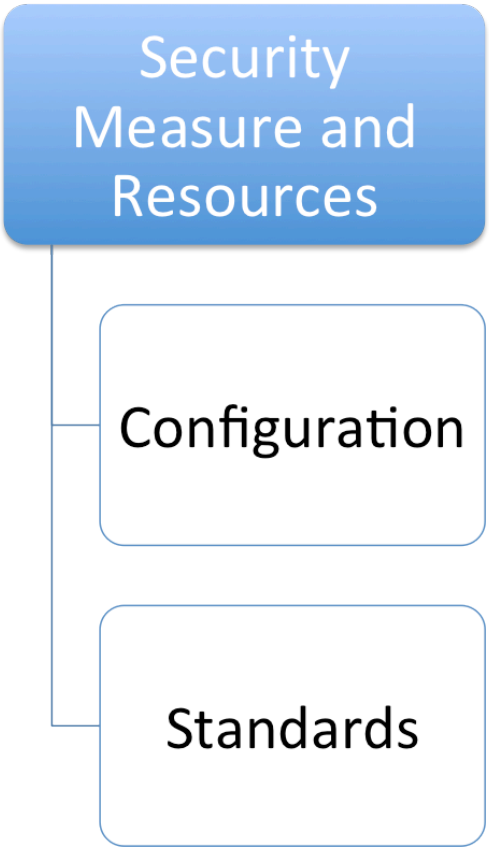


Figure 4.15: Security Measures and Resources framework

1. Configuration.

   This is refers to the base configuration of the system or systems from a security perspective, for example ensuring that critical security updates are applied, that remote access via the root account is not available for Unix based operating systems. To an extent it is how to apply security to a system and some of the tools used to do so. The configuration recommendations made within this project for the security model under construction will be a relatively short list of such available. It would not be possible to list every possible permutation of security settings and tools available to the systems of small medical practices unfortunately. Also, some brevity is required for this project due to space constraints. Thus the recommendations made should not be considered a complete nor even a definitive guide on such matters, the intention is to provide a sound core foundation of general security configurations in a manner that allows that foundation to be expanded upon and apply to the differing system specific points or differing small medical practices.

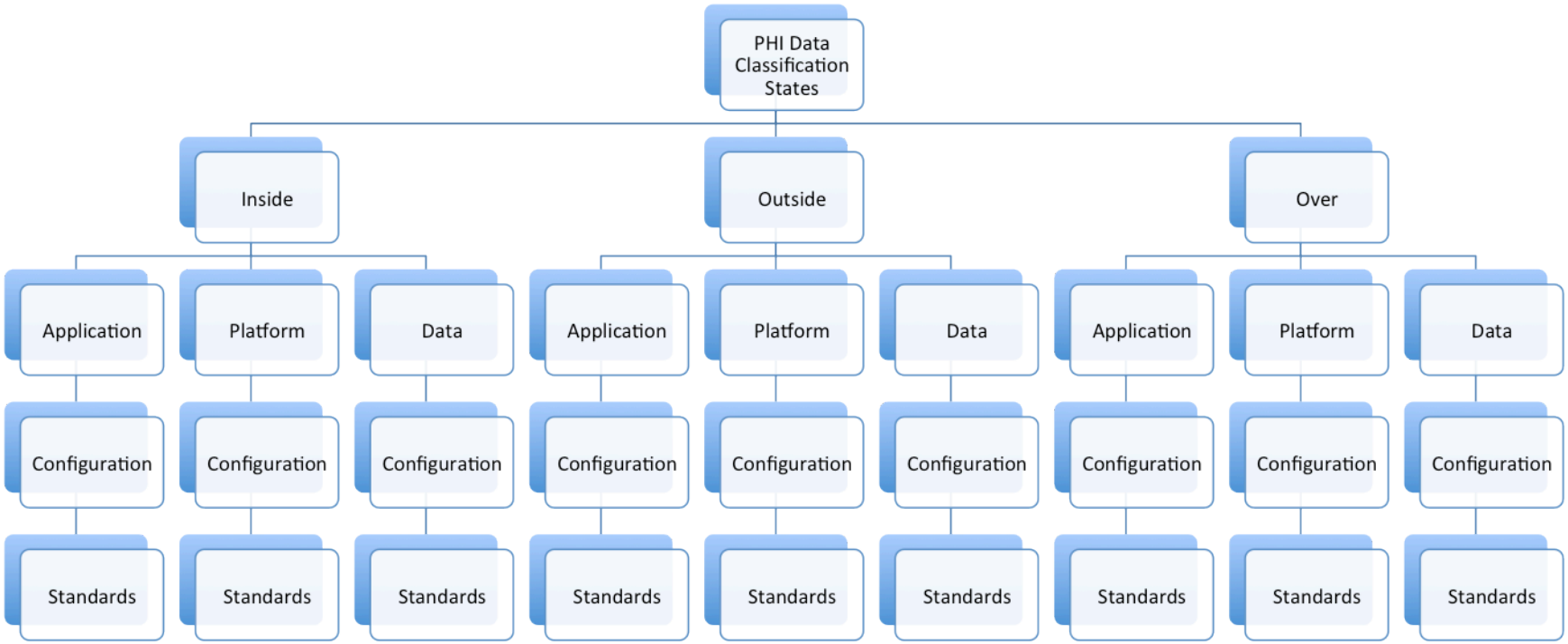
2. Standards.

   These are recognised standards and best practices for securing systems and services that are commonly used in small medical practice environments, for example the HL7 standard as referred to in chapter 3 would be an example of a standard that could be applied to an application service in an inside data state. They act as add-ons and plug-ins for this security model by providing a reference of more detailed information on the matter at hand. The standards used will not be an exhaustive list of those available and nor will they be the only option open to help secure the systems in question, there are a multitude of such documents available, any of which may be as valid as the others. However the ones used in this model will have the intention of at least meeting the need at hand and being valid enough to help ensure the security of the confidential PHI that is being protected.

Some of the configuration and standards resources that could be included in the application, platform and data classification's will be illustrated to aide the understanding of the problem domain that faces small medical practices. It should be noted that these are not a full list of the available or relevant materials and measures. There are a sample of such resources and in many instances some of the more desirable measures to implement.

There are a number of perspectives that could be taken when examining the individual classifications security measures and resources, including that of the software vendors engineering team and the systems administrator that is responsible for installing and maintaining the systems in question. Due to the nature of the relationships between vendors and systems administrators it may not always be possible for the systems administrators to perform all these recommendations though.

4.7 Complete Security Model Overview



4.8 Security Measures and Resources explained

4.8.1 Application

Configuration

- Software security development guides and best practices

  Many vendors provide guidance on how to develop software in a secure manner for their platforms, e.g. the Microsoft Security Development Lifecycle Process, (Microsoft, Unknown). Wherever possible, software should be developed in accordance with such guidance, if the medical practice can ascertain from the supplier if this has been done it will aide them in understanding the security posture of the application.

- Test products for security purposes
  Software testing is a crucial activity for software life cycle management; such testing should also include specific testing for security purposes when application developers are developing software that meets the "application" classification of this security model. The small medical practice should enquire from the supplier of the product if security testing was carried out on the product during its development.

  For the systems administrators who are responsible for installing the "application" software it may not be possible for them to test it to the maximum extent as they will have limited knowledge of the software and limited access to the source code. However, as far as practical it would be beneficial if they were to carry out security specific testing once the software is installed and when it is updated, Scarfone et al, (2008, C), provides some guidance on this.

- Code reviews for security purposes

Code reviewing is a practice whereby a third party reviews the source code for the “application” in question with a perspective for security. The systems administrator for a small medical practice is unlikely to have access to the source code of the “application”, unless it is an open source project or a custom made in house application, is limited in the extent to which they can carry out these actions. However the developers of the “application” system, particularly if it is designed to store and process PHI, should do so on a regular basis. Wherever possible medical practices should enquire as to whether such code reviews took place during the development of the application.

- Application Sandboxing and Application Firewalls

  Application firewalls act in a similar way to network firewalls, they segment the data flow around application processes and allow only certain interactions to take place. Sandboxing in software terms is similar to this but often implemented at the operating system level.

  Either or both of these security features will aide the “application” classified software security posture by restricting the access to a PHI related application, say a HIS, other processes and services have, thus reducing the threat surface applicable to the “application”. It would be advisable for systems administrators to utilise such defences when installing “application” classified systems and services if such is possible.

- Digitally Signed Software

  Signed software is that which has a security certificate applied to it to ensure its authenticity and that it has not been modified between release by the vendor and receipt by the customer. Wherever possible it would be useful for vendors to release software and updates in a signed manner as this provides assurances to those that are installing and running such software that it is authentic.

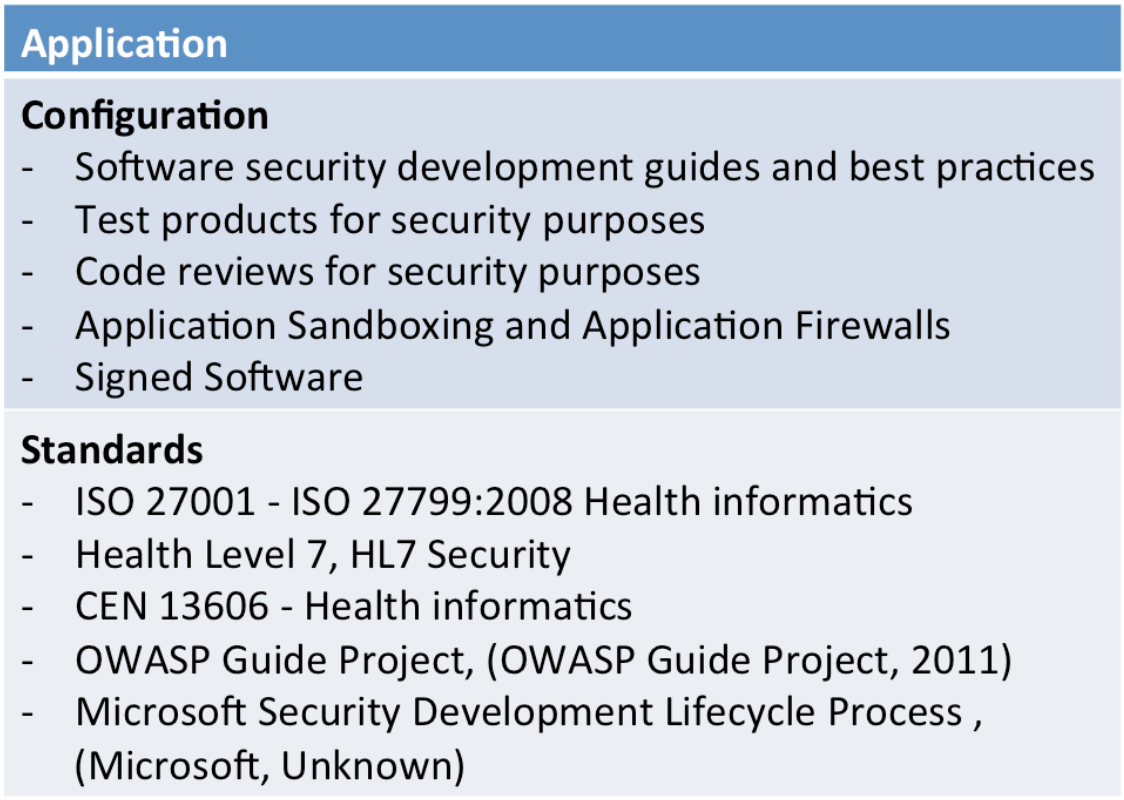


Figure 4.17: Application Resource Framework

Standards, as listed in bibliography

For matters such as those surrounding the use of HIS and EHR software standards can be very useful and assuring due to the sensitive nature of the PHI data that such software processes, as outlined in chapter three. If a product complies with a certain security standard then there is some certainty as to the secure nature of the product. Some standards, which were referenced in chapter three and can be used as guidance for applications that are specifically in the area of software for health informatics systems include:

- ISO 27001 - ISO 27799:2008 Health informatics
- Health Level 7, HL7 Security
- CEN 13606 - Health informatics
- OWASP Guide Project, (OWASP Guide Project, 2011)
- Microsoft Security Development Lifecycle Process , (Microsoft, Unknown)

4.8.2 Platform

Configuration

- Server and client host hardening

  Vendors may provide configuration guides and best practices for the products they supply, e.g. (Microsoft, 2006 - A), a Microsoft Exchange Server 2003 Security Hardening Guide. There is an onus for the systems administrators of small medical practices to ensure that any platform that hosts or processes PHI data complies with such best practices wherever possible

- Operating System Patch installation policy

  Operating system vendors regularly release security updates for their products. It is a crucial security posture that such patches are applied in a timely manner to ensure the security of the platform systems that host PHI in small medical practices.

- Line of business software patching policy

  Line of business or other applications such as HIS systems or other software that integrates with the systems and platforms where PHI resides and is processed in small medical practices may also have periodic security updates released for them. Timely installation of such updates is important in order to ensure the security posture of the platform in question.

- Anti Virus software installation and update policy

  Anti Virus software helps to prevent the intrusion of virus and other malicious software on client and server computers. Installation of a reputable anti virus

program and regular update of such is important to help ensure the security state of any network. It is also advisable to centrally manage such programs, so that instead of just relying on the automatic update feature built into the application, proactive steps are taken to check that such updates take place.

- OS level security technologies

  Many modern operating systems will include specific security technologies that are designed to harden and protect the system from attack and malicious interference, these technologies include:

  - Data-execution protection (DEP)
    DEP is designed to prevent an application from executing code in a memory space that is not indented to execute code, Microsoft, (2006 - B).
  - Address-space layout randomization (ASLR)
    Makes it more difficult for malicious code to guess or estimate the location of memory identifiers for other processes.

- File systems support file level security and encryption

  File level access controls can be applied to prevent un-authorised persons or systems from accessing data, which they have no right to see. This is an important requirement of any "platform" that stores PHI data to ensure that only those who should access it can.

  Encryption is the process whereby the plain text of the data to be protected has a cryptographic algorithm applied to it to transform it into a cypher text that it is not possible to understand without the cypher key that was used by the cryptographic algorithm to turn the plain text into a cypher text. It is important that platform systems that can store and process PHI data in small medical practices have the capability to encrypt such data if it is necessary to do so.

- Certificates for authentication, encryption and non repudiation

A digital certificate is a way to ensure trust between two or more systems and that sources of data are who they claim they are.

- Directory Service configuration

  A centralized and managed logon service is important for any organization. It helps to ensure that common security policies, such as password changes and strengths are globally enforced. Services such as Microsoft's Active Directory can also provide centrally managed configuration settings for client and server computers that are connected to the directory service which further improve the security posture of those computers.

- Client screen saver policy

  A simple way to suffer a data breach is to simply leave sensitive information visible on a computer screen that anyone may see. Ensuring that computer screens lock and require a password to unlock them when users are away from their computers will help prevent such potential breaches.

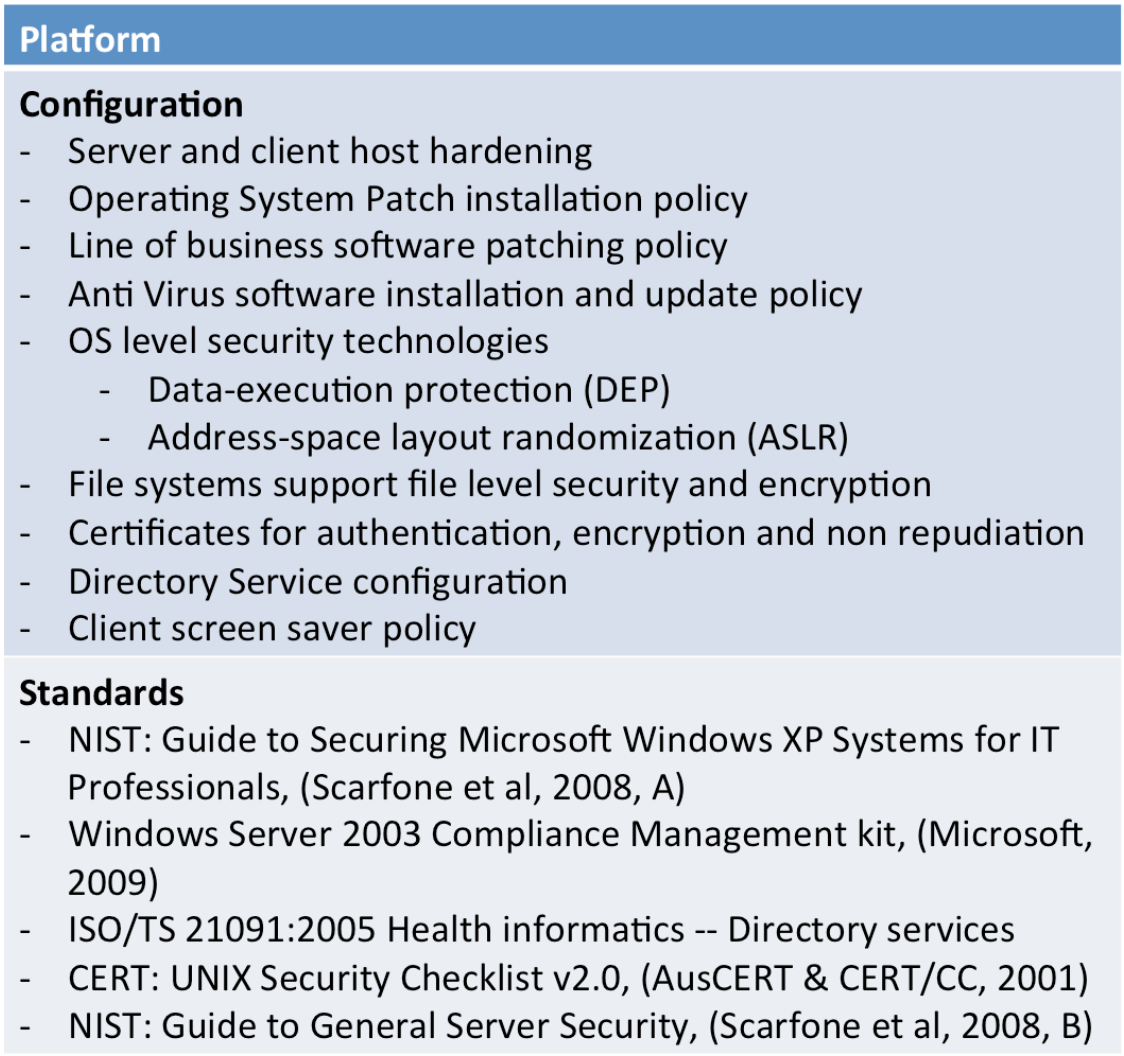


Figure 4.18: Platform Resource Framework

Standards, as listed in bibliography

- (Scarfone et al, 2008, A)
- (Microsoft, 2009)
- ISO/TS 21091:2005. Health informatics -- Directory services for security, communications and identification of professionals and patients
- (AusCERT & CERT/CC, 2001)
- (Scarfone et al, 2008, B)

4.8.3 Data

Configuration

- Physical access controls

  Physical access controls to the data itself and the mediums on which the data is stored are important to implement. These will include ensuring that physical records are stored in a secure location and that physical access controls such as locked doors are in place for the computers and storage media upon which the PHI data is stored.

- Access Level Controls for files and services

  It is important to ensure that restrictions on what PHI data users and other systems can access is based upon a strict "need to know" policy. If there is no requirement for a user or a system to have access to a particular data store then such access should not be granted. Granularity of such access is also important, if read only access is all that is required then that is what should only be provided.

- Where data is stored, including in the cloud

  Data can be stored in a number of locations and concerns can be raised if PHI is stored in inappropriate locations, these could include but not be limited to:

  - Cloud Storage and processing facilities. If data is to be stored and or processed offsite in a cloud environment strong consideration as to the ramifications and potential issues of this should be considered. (ENISA, 2009), provide a useful breakdown of both the risks and benefits of using such facilities and particular note through a case study of eHealth solutions for cloud computing. The report states:

> "*In some cases, it may be difficult for the cloud customer (in its role as data controller) to effectively check the data handling practices of the cloud provider and thus to be sure that the data is handled in a lawful way."*

A checklist that cloud computing customers can use for assurance of the protection of their data is provided and would be a useful document for small medical practices to use if they were to consider cloud computing facilities.

It should also be noted that employees may use cloud computing facilities themselves, e.g. online email services, that have the potential to store or process PHI data either through an "inside" or an "outside" data classification states without knowledge or consideration of the potential security risks. A policy and guidance should be put in place to educate staff of the potential risks of such.

- The PHI data of small medical practices could also be stored on removable and external storage media such as USB keys or CD ROMS. Policies and procedures are required to prevent such from happening. The only place that PHI data should be stored is within the "inside" data classification state of the systems a small medical practice may use, e.g. a HIS or EHR.

- Secure Erasure of data

When data has become end of life it should be securely erased. This would include soft copies of data, e.g. PHI records that are no longer required within the "inside" system, say for people that are no longer patients of the practice. But also for hard drives and other storage media that are being retired from use. Such storage media should be securely erased and the data on them destroyed.

- Data Backups

Special care needs to be taken of data backups. Say for example if a taped backup copy of the data base for the HIS of a small medical practice is stored offsite protective measures should be taken in such circumstances to ensure that while the availability portion of the confidentiality, integrity and availability paradigm is being maintained, so too is the confidentiality requirement of the PHI data in question preserved.

- Cryptography

Cryptography has already been explained in this chapter, but it should be noted that there are different levels and layers at which the cryptography can be applied as well as differing media and assets to which the cryptography should be applied to. These can include:

  - File level encryption
  - Full disk encryption, particularly for laptops
  - Encryption of backup media, tapes, hard drives
  - Encryption of portable media, CD's USB keys

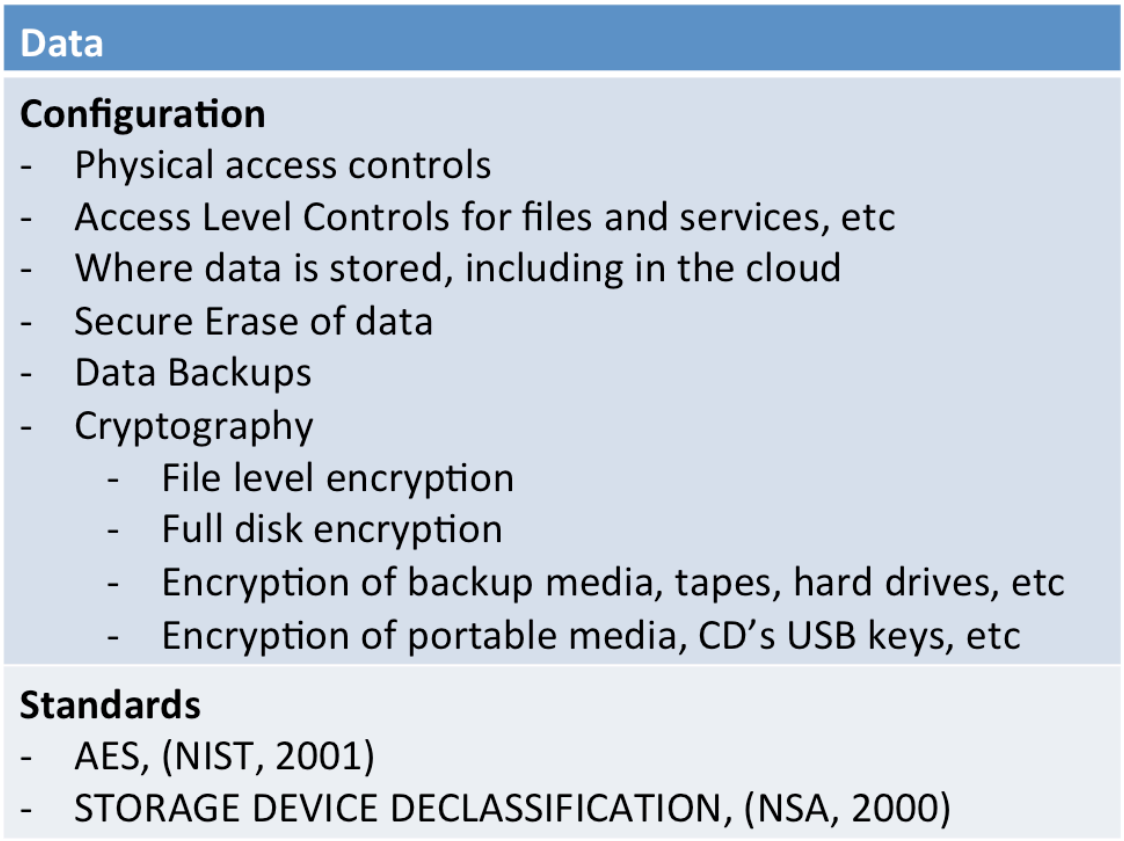


Figure 4.19: Data Resource Framework

Standards, as listed in bibliography

- (NSA, 2000)
- (NIST, 2001)
- (ENISA, 2009)

Over PHI Data Classification state, specific network use case

The "over" PHI data classification state applies to when data is transitioning between different data classification states, "inside and outside" and between differing systems and services classifications within and between the "inside and outside" states of this security model for small medical practices. This state includes the usage of networking facilities and equipment. While the "platform" component of the systems and services classifications could refer to matters such as router configuration hardening and

management of available networking services, the “application” component of the systems and services classification would apply to the services such as VPN and wireless network access that are available. As with much of the security model for small medical practices being presented as part of this project there is much replication and cross-pollination between these layers of “platform and application”. Some particular emphasis will be paid to networking facilities here though because of their importance and trusted nature within the environment of a small medical practice.

Configuration

- Firewall

  A firewall service running between the small medical practices network and the Internet is an important security practice to have in place. It will reduce the exposure of the PHI data contained within the network to risk of attack and access from outside the network.

- Router configuration

  It is important to ensure that basic configurations such as changing the default password on the router and updating the firmware and other software on it, as well as disabling all unnecessary services are carried out to reduce the threat vector that the network is exposed to.

- Network segmentation

  Dividing the network so that access between hosts is limited and restricted is an effective way to reduce the exposure of systems within the network. Say for example if a printer that was connected to the network was compromised or an attacker was spoofing the network address used by that printer but the printer was in a network segment that only allowed it to communicate over protocols that a printer would use, that would considerably reduce the attack surface available to the attacker.

- Separate logical networks for servers and clients

  Virtual Local Area Networks, VLAN's, would be used to achieve this. Restricting the servers and the clients from communicating with each other is an effective way of helping to protect the PHI data of the network, if only one segment is compromised that reduces the risk to the other segment.

- Host based firewalls

Host based firewalls are software firewalls that run on a client or server computer can be used in addition to a network layer firewall, they should not be used in place of one however. For example if it was not possible segment the network to separate the server from the client computers then a host-based firewall can be used in lieu of such network segmentation.

- Protection during transfer

It is important to protect the communication channel between systems that communicate PHI data to one another. If an attacker could gain access to the network it may be possible for them to intercept the PHI data passing between systems if it is in a plain text.

- SSL and TLS encryption

  These are the mechanisms employed to secure the hyper text transfer protocol, (http), if a web based service is used to pass the data between the systems this may be an appropriate security mechanism to employ.

- VPN

In the context of small medical practices, Virtual Private Networking is used to connect a remote host on an untrusted network to network of a small medical practice in a secure manner. If users are to work from home all such work should be done over a VPN connection.

- 802.1X Wireless

  The 802.1X standard is used to secure wireless communication. If a small medical practice is to use a wireless network then it should be protected using the Wi-Fi Protection Access, (WPA), protocol.

- IDS

  Intrusion Detection System's are used to monitor for and mitigate against remote attacks on a network and unusual and potentially hazardous traffic on the internal network. The are beneficial to use to help ensure that the network is not compromised and take action if an attacker is trying to compromise the network.

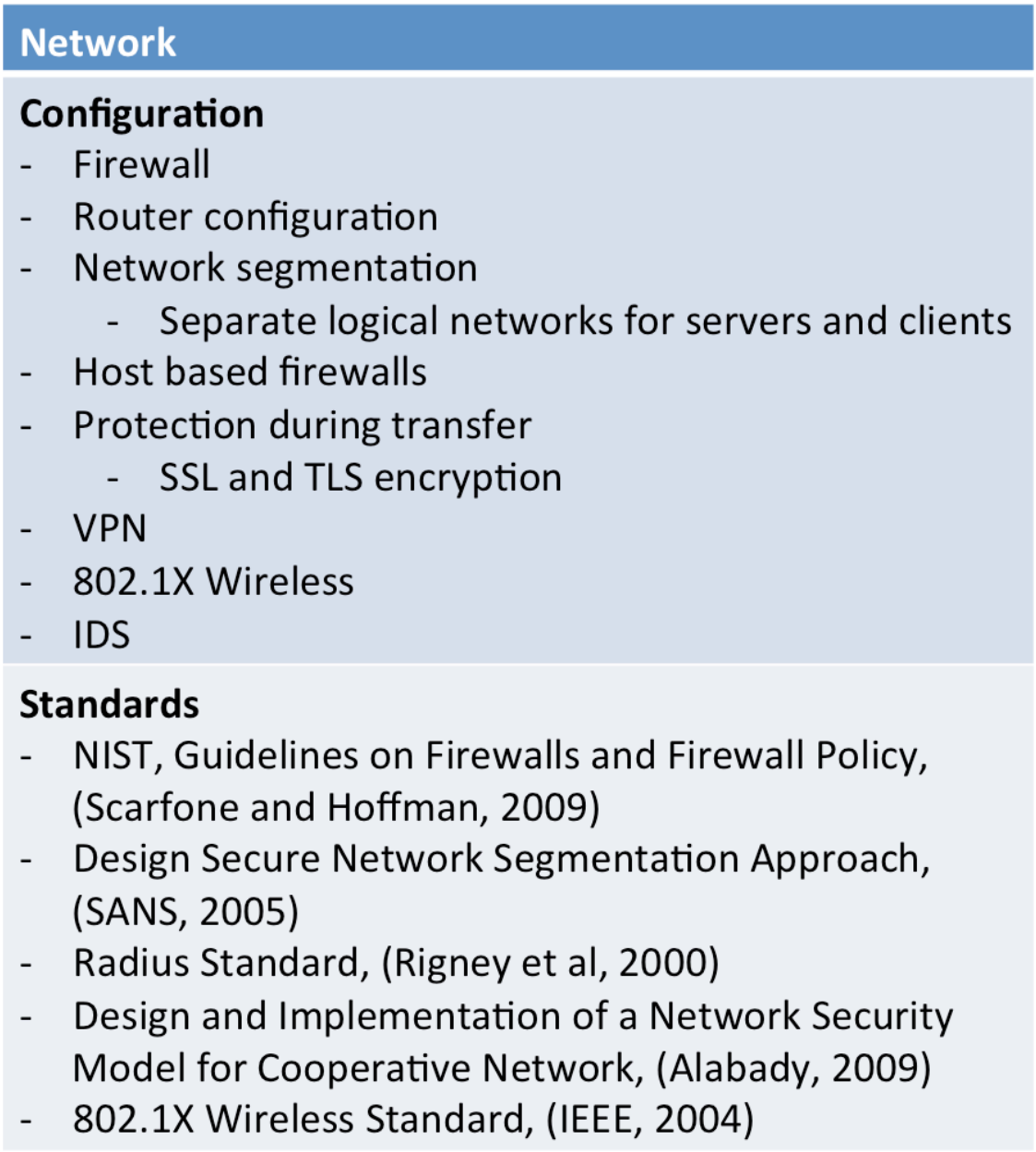


Figure 4.20: Network Resource Framework

Standards, as listed in bibliography

- (Scarfone and Hoffman, 2009)
- (SANS, 2005)
- (Alabady, 2009)
- (Rigney et al, 2000)
- (IEEE, 2004)

4.9 General rules and recommendations to follow

A short list of some general rules and recommendations to follow will be helpful. Many of these points are covered in some manner in the outlined security model but the following points are useful security mechanisms to employ regardless of what layer of the model they are implemented at.

Change management of systems and processes in place is important. When change is needed that may impact a system that stores or processes PHI data careful consideration of the overall security posture of the systems as a whole withing the small medical practice should be taken.
PHI data should not be stored on web servers or other servers that have direct access to the internet.
PHI Data should only reside on a system that is an "inside" system within the data classification model for this security model, e.g. a HIS system.
PHI data should not be stored on removable media such as USB keys or similar.
Wireless networks that can access PHI data should be encrypted, even if other security mechanisms such as transport level encryption is being employed

Figure 4.21: General rules and recommendations

4.10 Scope and limitations of the Security Model

With the states that PHI data can reside having been identified as "inside, outside and over", this will aide in identifying the critical systems and processes that the practice must protect and adhere to in order to help ensure the confidentiality, availability and integrity of the PHI that the practice stores and processes for its patients.

Once those systems are identified and categorised though it is necessary to be able to ascertain the state of security that they offer.

4.10.1 Limitations of the Security Model

A note of caution needs to be made at this stage that it is never possible to 100% guarantee the state of security of any system or data that resides within itself. As

Arthur, (2011), writes, "*Hacking is possible because modern computer systems are so complex that there will always be a flaw to be exploited somewhere*". This model will outline a method for helping to ensure the security and protection of PHI data for small medical practices, even the strictest possible adherence to this model cannot guarantee that security fully though unfortunately.

4.10.2 Scope of the Security Model

Looking at another framework that intends to help protect health information, Tulu & Chatterjee's, (2003), "A new security framework for HIPAA compliant health information systems", a detailed and extremely useful conceptual model is developed that addresses the technical and organisation issues needed to help protect health information in the context of the Health Insurance and Portability and Accountability Act's, (HIPAA), security rule. It details the stages of a framework intended to help management decide how to make their organisation HIPAA compliant. This model is extremely valuable but it does unfortunately have limited application to small medical practices. The requirement in such an environment is for a more applied, less high-level model.

This is because of the limited scope of organisations being catered for. Instead of a multitude of differing organisations and organisation types that can store and process PHI, the model being constructed for this model is dealing with a more homogenous subset of organisations in small medical practices. For example it is likely that the surveyed small medical practices will be using a single server computer to host their HIS as outlined in figure 2 of this chapter. It is also likely that the server will be running a Windows Server Operating System, which has almost 67% of market share according to one estimate, Wakabayashi, (2008). This provides benefits as it allows more specific's to be included in the security model that is being constructed.

4.11 Security Model Construction

These specifics can be included as add-ons to a more generalised base model that covers a wider domain to ensure the model is not however overly specific to become

un-helpful to practices unless they fit a very exact subset of systems. As an example of the more generalised base model take (Massachusetts 201 CMR 17.00), standards for data protection which outlines a broad approach to the duty's and standards required for protection of personal information in the Commonwealth of Massachusetts yet with some specific requirements and implementations. It outlines for example the requirements for computer system security which are very specific yet allow leeway in the implementation of the requirement:

> "*Encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly*"
>
> (Massachusetts 201 CMR 17.00)

These are specific requirements, that data, which is personally identifiable and is transiting any public and or wireless network must be encrypted, but it is general in that it does not specify the encryption system or algorithm to be used or the level at which it is to be encrypted. Imagine that a small medical practice had a wireless network over which computers could connect to the HIS. The practice would have the option of encrypting either the wireless network itself, using the WPA2 protocol perhaps, or the mechanism used to communicate with the HIS, the HTTPS protocol for example.

For the purposes of this model many of the specifics will take the form or standards or other published recommendations and best practices that are designed to increase the level of security of systems, take for example Microsoft's Windows XP Baseline Security Checklists[4] which aim to harden the Windows XP client operating system against attack. By using this approach the knowledge of experts in the area can be harnessed to further reinforce the protection systems being applied to the PHI processing and storing systems.

[4] Windows XP Baseline Security Checklists, available: http://technet.microsoft.com/en-us/library/cc751488.aspx, last accessed 27th of June 2011.

4.12 Limitations of application of the security model to the surveyed small medical practices

Due to the constraints of the primary research methodology, which is to conduct interviews with one or two people associated with the practice, it will not be possible to conduct in-depth investigations to comprehensively compare the surveyed practices against the designed security model. For example the CORAS method, (den Braber et al, 2007), of security analysis uses multiple workshops and meetings with differing personnel from the organisation being analysed. However such a method is designed for larger organisations than the small medical practices that this project is investigating.

Due to the restrictions of the time available to the interviewee's that agreed to be interviewed for this project it was not possible to conduct the investigation in such a detailed fashion. The approach this project will instead take is to conduct detailed interviews with key stakeholders in the small medical practices.

It is intended that these detailed interviews will provide valuable information, which can provide an accurate and adequate assessment of the practices compared to the security model. For example the OCTAVE® S approach for managing information security risks, which is a refined version of the full OCTAVE® approach designed for large organisations and then refined for small organisations in the OCTAVE® S approach, (Alberts et al, 2003), details a 3 phased approach for managing information security risks for small organisations.

Phase 1, building asset-based threat profiles, and phase 2, identifying infrastructure vulnerabilities can be conducted to an extent that allows for validation of the practice against the constructed security model through a significantly detailed interview of a person or persons with the necessary level of knowledge of the practice systems and procedures. Phase 3, developing security strategy and plans, is less appropriate for this project as the intention is to take a snapshot of the level of security within the practice when compared against the constructed security model by an external body and is not being done within the practice as a whole to improve on their current plans and strategies.

In order to build threat profiles and identify infrastructure vulnerabilities a method of classification and examination of the systems and services that store and process PHI data in small medical practices will be utilised based upon the outlined security model in this chapter.

4.13 Conclusion

This chapter has presented a technical and procedural security model that can be used to protect Personal Health Information in small medical practices and understand how that information is currently being protected in the survey practices.

Much repetition of security mechanisms and procedures is inherent in the outlined security model; this is not necessarily however a bad thing as it helps to ensure there are multiple layer's of protection.

With the security model outlined for small medical practices it will be possible to protect the PHI data that resides in such a practice as well as being able to ascertain and gauge the level of protection available in such practices.

5 EXPERIMENTATION & EVALUATION

5.1 Introduction

The experiment for this project was broken into two parts. Firstly a security expert validated the previously described security model. The second part was to use the security model to assess the level of data protection and computer security in a sample of small medical practices through qualitative research.

The first step, the validation by a security expert, of the two-step experiment was necessary to ensure that the designed security model was applicable and effective for the small medical practices and that it would provide an adequate way to apply security to and understand the security posture of the practices.

With the security model validated primary qualitative research could then be carried out to investigate the level of data protection in the surveyed small medical practices. This qualitative research was carried out by performing interviews with stakeholders in a number of small medical practices.

5.2 Experimentation

5.2.1 Experiment overview, data protection and computer security in small medical practices

The intention of this component of the experiment is to determine the level of data protection and computer security in small medical practices in Ireland when compared to the previously designed security model. To this end qualitative research was carried out in a number of small medical practices with an appropriate research methodology.

The experiment was simply to compare the protections applied to personal health information in the surveyed practices against the constructed security model for this project.

5.2.2 Research Methodology

The qualitative research methodology used was a structured interview methodology applied to relevant stakeholders in the small medical practices. A fixed set and sequence of predetermined questions was administered to the respondents and the respondents were given the option to see the questions in advance of the interview if they wished. The same set of questions was administered to all respondents.

5.2.3 Research Methodology Justification

This was necessary for a number of reasons. It was not expected that access to a large sample of medical practices would be available in order to administer a wide-ranging survey, thus the option to carry out interviews in order to obtain detailed information from the surveyed small medical practices was chosen. This would allow the questioning to be more detailed and also to allow the researcher to gauge the implicit understanding of data protection and computer security matters in small medical practices through meaning analysis of the question responses.

A structured interview methodology was also required due to the large amount of detailed information required to gauge a practices data security and protection posture against the security model outlined in the previous chapter.

Notes were taken of each interview and recordings were made as appropriate but not all respondents were willing to be recorded.

5.2.4 Interview design, linking the data received from the interviews to the security propositions in the security model

The constructed security model is a complex artefact that required detailed investigation in a small medical practice. To be able to ascertain the level of protection as per the Inside, Outside and Over data states model, while further iterating each data state into the application, platform and data systems classifications and then applying security measures and resources from the security model to each system and service is a large task.

In order to do so the logic applied to the interview structure was to divide it into two sections, the first was more focussed on data protection and other governance requirements; the second part was focussed on more technical aspects of computer security and data protection. That is not to say however that each section was exclusive of the other, for example the matter of requiring a password to unlock a computer was dealt with under the data protection and other governance requirements section, but such a protection is equally a technical protection as well. This structure was also chosen in order to separate the technical questions, which a non technical staff member in a medical practice, such as a practice manager, from the more technical questions that the non technical staff member would be less likely to answer. The more technical questions may need to be referred to a person with more technical knowledge of the practice.

Each section then had a number of sub sections that were designed to map and link the questions in the interview to components of the constructed security model. The methodology applied was to ask at least one question that applied to one security measure from the security model in chapter 4. Wherever possible questions were re-enforced in such a way that repeated the question, e.g. whether or not anti virus software was set to automatically update as well as a question asking if anti virus software was centrally managed in order to receive updates.

These repetition of questioning area's served as a control to ensure that the interviewee understood what was being asked and it also facilitated greater knowledge solicitation as it served to delve deeper into the understanding of the interviewee to the matter at hand. A full list of the questions posed to the respondents is available in the appendix. In total there were 100 items of unique information that were investigated in each practice.

5.2.5 Data Protection controls and security measures section

The following areas were investigated during the interview process in each small medical practice from the perspective of data protection and other governance matters. These areas map directly to the Data protection checklist for small medical practices established in chapter 2.

1. Are there documented procedural protections and policy compliance in place? For example were the
    - Registration with Data Protection Commissioner
    - Existence of a written internal data protection policy document
    - Defined and documented controls for deciding access levels to PHI
    - Whether there is a designated person who has responsibility for security and data protection
    - Existence of a data retention policy
    - Existence of a data subject access request policy
    - Existence of a data breach response plan

2. Computer account and PHI access controls
    - Password and screen locking policies
    - Computer account creation and termination procedures
    - Controls around leakage of PHI from its primary repository

3. Controls and protections applied to physical files

4. Staff training, understanding and control matters
    - Understanding of the legal environment associated with data protection in Ireland
    - Staff training in data protection matters
    - Contractual and other controls applied to staff to protect PHI
    - Understanding of future legislation and future concerns in regards data protection matters

5.2.6 Technical controls and security measures section

The following areas were investigated during the interview process in each small medical practice from a technical perspective. These area's originate directly from the security model designed in chapter 4 of this project

5. Assigned responsibilities for security matters
    - Responsibility for monitoring for vulnerabilities and ensuring backups complete and work
    - Responsibility for monitoring contractors and third party support companies

6. Inside data classification security measures
    - Security certification of HIS Application system
    - Responsibility for HIS maintenance
    - Ensuring that the HIS is the only data repository for PHI

7. Outside data classification security measures
    - Control of medical devices connected to the network
    - Control of other locations where PHI data may be stored, either intentionally or not
    - Control and management of data backups
    - Platform Security for Client computers
    - Platform Security for Server computers
    - Control of PHI data in cloud storage and processing facilities

8. Over data classification security measures
    - Secure Network design and segmentation
    - Wireless networking security
    - Destruction of data on devices that are no longer in use
    - Protection of data being transferred in offsite backups
    - Use of secure remote working facilities
    - Network monitoring for potentially malicious activity

5.2.7 Criteria for interpreting the findings

The concept of security metrics was considered but discounted. Security metrics have been defined as follows.

> "*Measurements provide single-point-in-time views of specific, discrete factors, while metrics are derived by comparing to a predetermined baseline two or more measurements taken over time*"
>
> Payne, (2006)

Because metrics are derived by comparison to a predetermined baseline and only one assessment was planned for each practice, it was not possibly employ them in this instance.

Criteria for interpreting the findings were still required though. It was decided to use a measure of adequacy for each individual piece of data pertaining to the data protection and computer security that was posed to the interviewee. That is to say, was the protection they described adequate to the task of ensuring the confidentiality, integrity and availability of the medical data they were charged with protecting?

This project will use the criteria of adequacy as defined in the constructed security model to assess the findings in the individual small medical practices surveyed. There will be three differing levels of adequacy used.

1. Not adequate, i.e. no protections are applied or the matter has not been considered.

2. Somewhat adequate, i.e. some protections are applied but could be improved upon. For example, in the case of polices and procedures, there may be an awareness within the practice as to the specific policy, (data subject access requests perhaps), but nothing may be formalised or documented on how to handle it in each case. This could be improved by documenting the formal process for such cases.

3. Adequate, the protections applied are enough to secure system, process, and policies which contain or control PHI data as per the constructed computer security model.

These definitions of adequacy will be applied to each of the questions posed to the interviewee.

5.2.8 Question Classifications

The questions will be categorised as per sections 5.2.5 Data Protection controls and security measures section and 5.2.6 Technical controls and security measures section to give a total of 8 question classification types. These types are:

1. Are there documented procedural protections and policy compliance in place? For example were the

2. Computer account and PHI access controls

3. Controls and protections applied to physical files

4. Staff training, understanding and control matters

5. Assigned responsibilities for security matters

6. Inside data classification security measures

7. Outside data classification security measures

8. Over data classification security measures

This categorisation and grouping leads to a number of easy to understand areas in which each of the practices and the practices as a whole can be assessed by comparison to the outlined security model. Each practice can also be assessed individually as a whole and for each of the categorisations above.

5.2.9 Questioning during the interview

A final note on the interview design was that the flow of the interview was not organised to match the outlined controls and security measures as they are detailed in this chapter. The questions were instead sequenced in such a way as to make them easier for the respondent to follow and the flow of the questioning does not map to the categorisation of the questions. All the points outlined in the control and security measures for the data protection and technical sections were examined by the interview questions, but not in the order presented here. Please see the appendix for the order the questions were posed in.

5.2.10 Stakeholders who were interviewed

In order to best understand the levels of data protection and computer security in the practices interviewed it was necessary to ensure that the stakeholder or stakeholders interviewed had sufficient knowledge of the practice management and technical aspects as possible. For this reason either the practice manager or one of the managing doctors was the person that was interviewed, at least in part.

There was potential for there to be issues with non-technicality of some of the stakeholders interviewed, for example a managing doctor of a practice may know how to use the systems in the practice but they may not have a detailed level of knowledge as to the administration of the systems. Because of this, where necessary questions were also posed to a stakeholder who had more knowledge of the technical side of the systems practices, such as the company that provide IT support for a practice.

5.2.11 Limitations of research methodology

When a large scale security audit is run in any environment more than one or two interviews will be conducted in order to fully understand the complete security posture of the environment, for example the CORAS Method, (den Braber et al, 2007), uses 7 phases of detailed analysis when performing risk analysis and audit tasks. Also other methods such as site visits and examinations where the investigator takes a more detailed and proactive look at the facilities in the environment would be appropriate ways of gauging the security posture of an environment.

Such methods were however discounted for this project though. This was because of the limited time that the respondents had to partake in the research and also because those more intrusive methods may not have been well received and meant that the respondents were more disinclined to participate in the research. A balance was needed between what could be attained by the investigator and the level of participation the respondents were willing to provide.

Because of this it was not possible to gain a complete technical overview of the practices that were surveyed and as such the interviews that were conducted should be considered more akin to a first iteration or pass of a more detailed investigation or audit. It is hoped though that the results received indicate a fair representation of the state of data and computer security in the surveyed practices.

5.2.12 Details of the practices where interviews were carried out

A total of four small medical practices contributed to the primary research for this project. Identifiable details of these practices cannot be provided in order to preserve their anonymity but a brief description of each is appropriate. All practices were located in the greater Dublin area.

1. This practice provided care for more than 8000 patients. This care was provided by 5 general practitioners, 3 nurses and supported by 5 administrative staff. This practice was unique amongst the others interviewed as the Health Service Executive, HSE, provided its IT facilities.

   The Practice Manager was interviewed in the first instance and they were unable to provide detailed enough answers to some of the technical

questions, so a follow up phone interview was carried out with a member of staff of the HSE's Information and Communications Technology services.

2. The second practice has more than 13000 patients, with care being provided by 5 general practitioners, 2 nurses and supported by 5 administrative staff. This practice was a stand alone GP practice

   The primary interview was carried out with one of the managing general practitioners of the surgery and a follow up phone interview was carried out with a member of staff from the technical support company that provide IT services to the surgery for the more technical aspects of the investigation.

3. This practice provided care to about 3500 employees of a larger organisation whose main focus was not health care. The care was provided by 4 general practitioners, 3 nurses, 4 pharmacists and supported by 4 administrative staff. As mentioned this practice is part of a larger organisation and many of its data protection initiatives originate from that organisation.

   The interview was carried out with the Administrative Manager of the surgery. There was no need for any follow up interview with a more technical person, as the administrative manager was able to adequately answer the technical questions.

4. The final practice did not divulge the number of patients or staff associated with it. It is also part of a larger organisation whose primary focus is not health care.

   Due to the large nature of the organisation with differing offices and departments being responsible for different matters pertaining to security and data protection in the organisation, written responses to the questions were provided by the different offices and departments, no interview was carried out in this instance.

The numbers 1 to 4 from the description above will be used to identify the individual practices as they are referenced further in the text.

5.3 Evaluation of the security model by a security expert

The first step in the evaluation was to have the security model itself validated. Mr Darren Fitzpatrick, an Information Risk and Compliance Consultant at Espion Intelligence carried this out.

5.3.1 Comments from the security expert

The full comment thread with the security expert can be found in the appendix. The following were the main points from the correspondence in respect to the security model contained in chapter 4 of this document.

> "Given the guidance provide using the concepts of systems and services classifications, their relevant security measures and resources and the 'state' in which data is secured, I would be happy to describe the model as valid. The model, in its current state seems conceptually sound as the foundations of a usable security model for PHI in small medical practices"
>
> Darren Fitzpatrick, (2011)

Based on this the security model was deemed to be valid to ensure the protection of personal and protected health information in small medical practices in Ireland.

The designed security model was not perfect however, the security expert made the following valid and useful comments.

1. Always look at the issue from the perspective of the person implementing it.
2. Be more definitive about the security measures to be used, instead of recommending that they could be carried out, insist that they are necessary in order to comply with the standard.

Due to the time constraints of the project it was not possible to incorporate these recommendations into the model. If the designed security model is to be used as the basis for any further work these recommendations should be considered.

5.4 Evaluation of data protection and computer security in the small medical practices

The results from the full interview question process can be found in the appendix. These findings will be summarised here to gain a better understanding of the state of data protection and computer security in the surveyed small medical practices.

5.4.1 Overall evaluation of data protection and computer security in the surveyed small medical practices

Overall the results of the investigations carried out to assess the level of data protection and computer security in the surveyed small medical practices were positive. When compared to the model the practices surveyed were found to be largely in compliance with the security model. There were some areas of concern and they will be listed separately but as a whole the levels of confidentiality, integrity and availability in the surveyed practices were found to be adequate when compared to the security model.

Some area's that showed particularly positive results were the protection levels applied to the "Outside" and "Over" data classification states from the security model. The technical protections applied to the "Application", "Platform" and "Data" system and services classifications were on the whole adequate to ensure the protection of the personal health information in surveyed medical practices.

It is also worth noting that one particular security measure in place for the "Over" data classification state was that only one of the practices surveyed employed a wireless network and adequate protection measures were applied to that network.

5.4.2 The implicit understanding of data protection matters in the surveyed practices

When analysis of the meaning of the respondent's response to the questions was interpreted it became clear that there was an implicit understanding of data protection matters in the surveyed practice. Each respondent took the issue seriously. Some examples of this included the following.

The practice manager for Practice 1 stated, "*it is everyone's responsibility*" when talking about who was responsible for security in the practice. They also commented on the use of a PPS number as a unique identifier for the Cervical Cancer screening website[5] and raised concerns about the use of a persons PPS number for such.

[5] CervicalCheck - The National Cervical Screening Programme, www.cervicalcheck.ie last accessed 21st of June, 2011

One of the owners of Practice 2, when discussing the access that administrative staff has to the practices HIS commented, "*Confidentiality is implied as part of the job*". Further they discussed an issue whereby a data breach of personal health information almost took place. The respondent was quite concerned by this and commented on the seriousness of the matter even though the breach had not occurred. Another case was raised whereby records were mixed up and a letter containing personal health information was sent to the wrong patient. That incident lead to the implementation of a written policy for issuing patient information in the practice

The administrative manager for Practice 3 stated that access to health information was granted on a "*need to know basis*" when staff members were being setup with to access to the practices HIS. In addition, while no specific training in data protection matters was given to staff at the time of the interview, the administrative manager was planning a talk from a data protection professional that would be mandatory for all staff. The importance of data protection was further highlighted when the administrative manager mentioned the problem with having a conversation pertaining to health information in an area that was accessible to the public.

5.4.3 Area's of concern for security and data protection

The following areas were of some concern as in general the findings were that the levels of control and protection applied in the practices as a whole were not adequate.

Only half of the surveyed practices had a written data protection policy and those were the practices that were part of a larger organisation that maintained a data protection policy for the organisation as a whole. However this matter is somewhat mitigated by the inherent understanding of the need for data protection in the practices as a whole.

There are concerns with the level of access that administrative staff gets to personal health data. While all respondents stated that such access was necessary for the staff to perform their duties, only one responded that their administrative staff could only view and not modify the personal health information contained in their HIS.

There is scope for formalised training of staff in the area of data protection, while the implicit understanding of data protection is good, there was no specific data protection training taking place in the surveyed practices.

Another area of general weakness was the monitoring of the devices connected to the practices network for vulnerabilities such as security patches that need to be applied. There was scope for the improvement of this. Also, there was a lack of an intrusion detection system in at least half of the surveyed practices.

The majority of the client computers that connected to the networks of the small medical practice were running Windows XP, as per (National Security Agency, 2011), and echoed in the security model constructed in chapter 4 of this document, it is advisable that practices upgrade to Windows Vista or Windows 7 operating systems.

None of the server computers that the small medical practices used employed any disk level encryption protections. However, this failing against the security model was mitigated with the fact that strong physical access controls were in place for all the practices and that all the practices took the destruction of data on retired storage media seriously. Another potential risk to medical practices was that those with a smaller network that was not part of a larger organisation did not employ network segmentation techniques to isolate their servers.

5.4.4 Findings broken down by question categorisation

Documented procedural protections and policy compliance matters.

The procedures and practices in place for compliance were generally adequate. An area that could be improved on in general was that of a written data protection policy and a written policy for deciding the level of access that staff requires to PHI.

Computer account and PHI access controls.

Overall the controls applied to computer accounts and access to PHI was very rigorous and adequate to meet the requirement to protect the PHI in place. This was one of the better areas of compliance with the security model.

Controls and protections applied to physical files.

In general the protections and controls applied to physical files are categorised as being somewhat adequate for data protection purposes. In this area there is room for improvement for by example ensuring that physical files are maintained in a more secure environment.

Staff training, understanding and control matters

Staff training for data protection could be improved in general. On the whole the protections and measures taken were somewhat adequate but there was considerable scope for improvement. The implicit understanding evident in the practices of data protection should mitigate this, but as was quoted in one of the examples from a practice, there is potential for a problem here.

Assigned responsibilities for security matters

This was very much a mixed bag; there is an understanding that such matters should be assigned for some-ones attention but the understanding of the specifics, such as vulnerability monitoring was not evident from the analysis of the interviews carried out with the non-technical practice managers and similar staff.

Inside state data classification security measures

Overall the technical protections applied to the “Inside” data classification state are somewhat adequate. There are some matters for concern as there is uncertainty as to whether transport level communication protections such as end-to-end encryption are applied to communications between HIS applications and client computers. While this problem could also be categorised into the “Over” data state classification it is being

dealt with here as such a change would probably require modification of the HIS application.

Also, it is unclear if the health information systems that the practices utilise comply with the security standards specified in the security model. Investigations were carried out to try to determine this, including contacting a leading provider of HIS software in Ireland, but it was not possible to determine either way if the software in the surveyed practices meets the security standards or not.

Outside state data classification security measures

The "Outside" data classification state was very well protected to an adequate or somewhat adequate level. This was very encouraging as much of the attack surface for access to PHI comes from "Outside" systems such as client computers being infected with malware that puts the PHI at risk and while the protections were not perfect, one practice could implement a better policy for patching client computer systems for example, the results were encouraging.

Over state data classification security measures

The "Over" data classification state was generally also well disposed for security measures, area's that could be improved included implementing segregation of the network that the server computers were connected to in some of the practices.

5.5 Conclusion

This chapter has outlined the methodology by which the experiment was conducted along with the results of the experiment.

The constructed security model was found to be valid by the security expert that who analysed it.

Overall the level of technical security protections in the small medical practices was found to be adequate. This was contrasted with the procedural data protection matters,

which while still mostly adequate, were not as well catered for as the technical matters. This was however mitigated by a deep underlying understanding of the necessity for privacy and data protection in the small medical practices.

6 CONCLUSION

6.1 Introduction

The purpose of this project was to construct a valid security model and then use it to determine the state of data protection and computer security in small medical practices in Ireland. The findings were that in general the security and data protection measures in the surveyed practices were adequate to ensure the confidentiality, integrity and availability of the personal health information that is entrusted to the small medical practices. There were some areas that required further coverage by the practices and these were noted. The security model would aid the practices in rectifying those deficiencies.

6.2 Research Definition & Research Overview

The area of interest for the research in this project was that of data protection and computer security. It focused specifically on applications of these two matters to small medical practices, while retaining a broad enough scope to prevent any other relevant material from being left out. The literature at hand was not found to be fully adequate for small medical practices purposes.

The secondary research for this project was divided into two parts. A specific governance section focusing on data protection legislation and guidance and a computer security section that covers the measures and standards needed to secure systems that contain personal health information. In neither section was an approach found which took the same form as the model in this project, nor were the exact requirements and methods of this project met in any of the other surveyed literature.

6.3 Contributions to the Body of Knowledge

This project aims to contribute two things to the body of knowledge. Firstly a valid, unique security model that can be used to assess the level of data protection and computer security in a small medical practices.

Secondly it provides an assessment of the level of data protection and computer security in the surveyed small medical practices. This level of protection has been found to be adequate.

6.4 Experimentation, Evaluation and Limitation

The experiment first validated the security model and then applied it to the surveyed small medical practices to gauge the levels of data protection against the model. The experimentation was successful. The security model was found to be valid from a security perspective and the model was applicable to the surveyed practices. Also the level of data protection as described by the model overall was adequate in the surveyed small medical practices.

There is the potential for bias in the findings because the respondents who were willing to participate in the study may be more likely to have an interest and concern for the area of data protection in their practices than a more random set of potential respondents. Also, the data set was of a limited size, only four practices were assessed, therefore it could not be said to be representative of the area as a whole.

In addition the representative sample of small medical practices had a larger proportion of practices that existed within a larger parent organisation. This sampling was accidental and not intended; it was simply the way that it worked out. This sampling could be problematic, as it does not represent a large enough cross section of independent medical practitioners who are not part of a larger parent organisation yet still store and process medical data for their patients.

6.5 Future Work & Research

In future work the security model could be refined more, particularly along the lines that the security expert suggested, making it more authoritative and requiring the practices to take actions instead of suggesting they do so.

Further research could be carried out from a larger data set, if possible a data set that was more random and less inclined to pay data protection specific attention. The research could also be taken into larger medical organisations such as hospitals.

It may also be helpful to target any further research specifically at stand-alone medical practices that are not part of a larger organisation as such practices are less likely to have the large scale facilities and support structure that are available to practices who are part of a parent organisation.

Further work is also needed in the area of the health information systems in use in the practices. The constructed security model specifies security standards that could apply to the HIS as well as development practices such as code reviews that can be carried out to determine the level of security in the applications. It would be beneficial if such a study could be carried out.

6.6 Conclusion

If the findings of this project are representative of the state of data protection and computer security across small medical practices as a whole in Ireland then the implications for the patients who entrust their data to the practices are positive. While there are some shortcomings, overall the level of protection of that data is adequate. This also applies to a policy viewpoint as those in positions of governance have an assurance that their requirements are being met. It is not however possible to determine if this is the case though without further investigation.

However from a policy perspective there is an initiative that could make the efforts of this project moot. If a unique health identifier was to be implemented, (Health Information and Quality Authority, 2009), and a Central Rerecords Systems, (CRS), that was hosted and administered by a central service provider retained and stored the personal health information of the patients, there would no longer be an onus on the individual practice to maintain and secure their own medical records. This service would be provided by another body and assuming that such a service were secure, the constructed security model in this project could at least start as a foundation to assure the security of such a system, there would be benefits to the medical practices no longer having to maintain their own records. This would be a better way to ensure the confidentiality, integrity and availability of personal health information for small medical practices in Ireland than each practice maintaining their own records.

BIBLIOGRAPHY

Aceituno, V. (2005). On Information Security Paradigms. The ISSA Journal. September

Alabady, S. (2009). Design and Implementation of a Network Security Model for Cooperative Network. International Arab Journal of e-Technology. 1 (2), p26-36.

Alberts, C, Dorofee, A, Stevens, J, Woody, C. (2003). Introduction to the OCTAVE® Approach. Available: www.cert.org/octave/approach_intro.pdf. Last accessed 27th June 2011

Anderson, R.J.. (1996). A security policy model for clinical information systems. Security and Privacy, 1996. Proceedings., 1996 IEEE Symposium on. p30-43

Arthur, C. (2011). How computer hackers do what they do ... and why. Available: http://www.guardian.co.uk/technology/2011/jun/06/hackers-how-and-why-they-hack. Last accessed 27th June 2011.

BBC. (2008). Up to 15,000 patients' data taken. Available: http://news.bbc.co.uk/2/hi/uk_news/england/hampshire/7608000.stm. Last accessed 7th of June, 2011.

Bell, D. E. and LaPadula, L. J. (1973). Secure Computer Systems: Mathematical Foundations. MITRE Technical Report 2547, Volume I

Blobel B & Roger-France F. (2001). A systematic approach for analysis and design of secure health information systems. *International Journal of Medical Informatics*. 62 (1), 51-78.

Blobel B, Pharow P and Roger-France F. (1999). Security Analysis and Design Based on a General Conceptual Security Model and UML. HIGH-PERFORMANCE COMPUTING AND NETWORKING. 1593/1999, 919-930.

Blobel, B. (2004). Authorisation and access control for electronic health record systems. International Journal of Medical Informatics. 73, 251—257.

Bright, P. (2011). Anonymous speaks: the inside story of the HBGary hack. Available: http://arstechnica.com/tech-policy/news/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack.ars. Last accessed 10th of July 2011.

Brook, C. (2011). UCLA Health Services Pays $865K, Settles HIPAA Violations. Available: https://threatpost.com/en_us/blogs/ucla-health-services-pays-865k-settles-hipaa-violations-070811. Last accessed 10th of July 2011

CEN 13606 - Health informatics . (2011). CEN 13606 - Health informatics . Available: http://www.en13606.org/. Last accessed 4th of July 2011.

Centre for Disease Control and Prevention. (2003). HIPAA Privacy Rule and Public Health Guidance from CDC and the U.S. Department of Health and Human Service. Available: http://www.cdc.gov/mmwr/preview/mmwrhtml/m2e411a1.htm. Last accessed 7th of June, 2011

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (European Treaty Series, No. 108)

Council of Europe, Committee of Ministers. Recommendation No. R (97) 5 of the Committee of Ministers to Member States on the Protection of Medical Data.

Darren Fitzpatrick. darren.fitzpatrick@espion.ie. RE: Security Model - Thoughts. 14th of July 2011.

Data Protection (Amendment), 2003

Data Protection Act, 1988

DATA PROTECTION ACTS, (1988). DATA PROTECTION ACT, 1988.Available: http://www.irishstatutebook.ie/1988/en/act/pub/0025/index.html. Last accessed 8th January 2011.

Data Protection Commissioner. (2011). Data Protection Acts 1988 and 2003 A Guide For Data Controllers. Available: http://www.dataprotection.ie/documents/forms/NewAGuideForDataControllers.pdf. Last accessed 28th of March 2011.

Data Protection Commissioner. (n.d.). The Data Protection Rules. Available: http://www.dataprotection.ie/docs/The_Data_Protection_Rules/21.htm. Last accessed 7th of June, 2011.

Data Protection Commissioner. (Unknown). A Guide for Data Controllers. Available: http://www.dataprotection.ie/docs/a_guide_for_data_contollers/696.htm. Last accessed 7.

den Braber, F, Hogganvik, I, Lund, M S, Stølen, K and Vraalsen, F. (2007). Model-based security analysis in seven steps — a guided tour to the CORAS method. BT Technology Journal. 25 (1), 101 - 117.

Department of Health & Royal College of General Practitioners. (2005). Good practice guidelines for general practice electronic patient records (version 3.1). Available: http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4008657. Last accessed 7th of July 2011.

Department of Health and Children. (2008). DISCUSSION PAPER ON PROPOSED HEALTH INFORMATION BILL . Available: http://www.dohc.ie/consultations/closed/hib/discussion_paper.pdf?direct=1. Last accessed 7th of June, 2011

Department of Health and Human Service. (2003). 45 CFR Parts 160, 162, and 164 Health Insurance Reform: Security Standards; Final Rule. Available:

http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityrulepdf.pdf. Last accessed 6th of July 2011

Department of Health and Human Service. (2010). PART 164_SECURITY AND PRIVACY--Table of Contents, Subpart E_Privacy of Individually Identifiable Health Information. Available: http://frwebgate.access.gpo.gov/cgi-bin/get-cfr.cgi?TYPE=TEXT&YEAR=current&TITLE=45&PART=164&SECTION=512. Last accessed 6th of July 2011.

Directive 1999/5/EC of the European Parliament and of the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity

Drummond D. (1), (2010). A new approach to China. Available: http://googleblog.blogspot.com/2010/01/new-approach-to-china.html. Last accessed 7th of June, 2011.

Electronic Health Record Communication (EN 13606)

EU Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

European Network and Information Security Agency (ENISA). (2009).*Cloud Computing, Benefits, risks and recommendations for information security*. Available: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment. Last accessed 4th of July 2011.

Fonseca, Brian. (2008). Thieves pilfer backup tapes holding 2M medical records. Available: http://www.computerworld.com/s/article/9080322/Thieves_pilfer_backup_tapes_holding_2M_medical_records . Last accessed 7th of June, 2011.

General Practice Information Technology Group. (2008). No Data No Business. Available: http://www.icgp.ie/go/in_the_practice/information_technology/news_updates/E3E7417C-19B9-E185-833C5534D98B3B8C.html. Last accessed 7th of July 2011.

Goodin, D. (2011). (B). Citigroup hack exploited easy-to-detect web flaw. Available: http://www.theregister.co.uk/2011/06/14/citigroup_website_hack_simple/. Last accessed 10th of July 2011.

Goodin, D. (2011). (C). Stolen RSA data used to hack defense contractor. Available: http://www.theregister.co.uk/2011/06/06/lockheed_martin_securid_hack/. Last accessed 20th of June, 2011.

Goodin, Dan. (2011). (A) User data stolen in Sony PlayStation Network hack attack. Available: http://www.theregister.co.uk/2011/04/26/sony_playstation_network_security_breach/. Last accessed 7th of June, 2011.

Health Information and Quality Authority. (2009). Recommendations for a Unique Health Identifier for Individuals in Ireland. Available: http://www.hiqa.ie/content/recommendations-unique-health-identifier-individuals-ireland. Last accessed 15th of July 2011.

Health Insurance Portability and Accountability Act. 1990

Health Level Seven International. (2005). Security. Available: http://www.hl7.org/Special/committees/secure/overview.cfm. Last accessed 20th of June, 2011.

HIMMS. (Unknown). Electronic Health Record. Available: http://www.himss.org/ASP/topics_ehr.asp. Last accessed 20th of June, 2011.

HL7, Health Level Seven International. (2005). Security. Available:

http://www.hl7.org/Special/committees/secure/index.cfm. Last accessed 4th of July 2011.

ICGP/GPIT Data Protection Working Group. (2011). A Guide to Data Protection Legislation for Irish General Practice. Available: http://www.icgp.ie/speck/properties/asset/asset.cfm?type=Document&id=B1CF543F-19B9-E185-838EA8A4A14F9E84&property=document&filename=ICGP_Data_Privacy_Doc.pdf&revision=tip&mimetype=application%2Fpdf&ap. Last accessed 7th of July 2011.

IEEE. (2004). 802.1X - Port Based Network Access Control. Available: http://www.ieee802.org/1/pages/802.1x.html. Last accessed 4th of July 2011.

Irish Health. (2008). HSE admits data protection breach. Available: http://www.irishhealth.com/article.html?id=10110&ss=data. Last accessed 7th of June, 2011.

Irish Health. (2009). Stolen HSE laptop had sensitive data. Available: http://www.irishhealth.com/article.html?id=15690&ss=data. Last accessed 7th of June, 2011.

Irish Health. (2010). HSE told to improve data security. Available: http://www.irishhealth.com/article.html?id=17141&ss=data. Last accessed 7th of June, 2011.

Irish Times. (2009). 8,000 NI patients' medical records missing. Available: http://www.irishtimes.com/newspaper/breaking/2009/0127/breaking55.htm. Last accessed 7th of June, 2011.

ISO 27799:2008 Health informatics — Information security management in health using ISO/IEC 27002

ISO IEC 27799 2005 – Information technology — Security techniques — Code of practice for information security management

ISO TC 215 Health Informatics

ISO/IEC 27001:2005 - Information technology -- Security techniques -- Information security management systems – Requirements

ISO/TS 21091:2005. Health informatics -- Directory services for security, communications and identification of professionals and patients

IT Security Office, Trinity College Dublin. (2005). Key Requirements of Secure Systems. Available: http://www.tcd.ie/ITSecurity/software/keyreq.php. Last accessed 7th of July, 2011.

Johnson, E. (2009). Data Hemorrhages in the Health-Care Sector1. Available: http://fc09.ifca.ai/papers/54_Data_Hemorrhages.pdf. Last accessed 7th January 2011

Johnson, E. (2009). Data Hemorrhages in the Health-Care Sector1. Available: http://fc09.ifca.ai/papers/54_Data_Hemorrhages.pdf. Last accessed 7th January 2011.

Kalra, D. (2006). Electronic Health Record Standard. IMIA Yearbook of Medical Informatics 200. 139-144.

Kenisberg N, Faurbech K, McMillan M. (2004). A framework for HIPAA it HIPAA compliance. EDUCASE Centre for Applied Research. 25, 1-13.

Kleef, M. (2009). Security Compliance Management Toolkit released. Available: http://blogs.technet.com/b/mkleef/archive/2009/03/12/security-compliance-management-toolkit-released.aspx. Last accessed 10th fo July 2011.

Massachusetts 201 CMR 17.00: STANDARDS FOR THE PROTECTION OF PERSONAL INFORMATION OF RESIDENTS OF THE COMMONWEALTH, available http://www.mass.gov/Eoca/docs/idtheft/201CMR1700reg.pdf, last accessed

27th of June 2011

McGraw-Hill Concise Dictionary of Modern Medicine. (2002). Health Information System. Available: http://medical-dictionary.thefreedictionary.com/health+information+system. Last accessed 20th of June, 2011

McKenzie, P. (2011). Weapons of Mass Assignment. Communications of the ACM. 54 (5), 54-59.

Mearian, Lucas. (2011). U.S. patients trust docs, but not e-health records, survey shows. Available: http://www.computerworld.com/s/article/9210061/U.S._patients_trust_docs_but_not_e_health_records_survey_shows. Last accessed 7th of June, 2011.

Microsoft. (2006 - A). Microsoft Exchange Server 2003 Security Hardening Guide. Available: http://www.microsoft.com/download/en/details.aspx?id=8055. Last accessed 4th of July 2011.

Microsoft. (2006 - B). A detailed description of the Data Execution Prevention (DEP) feature in Windows XP Service Pack 2, Windows XP Tablet PC Edition 2005, and Windows Server 2003. Available: http://support.microsoft.com/kb/875352/EN-US/. Last accessed 4th of July 2011.

Microsoft. (2009). Windows Server 2003 Security Guide. Available: http://www.microsoft.com/download/en/details.aspx?id=8222. Last accessed 4th of July 2011.

Microsoft. (Unknown). Microsoft Security Development Lifecycle Process . Available: http://www.microsoft.com/security/sdl/default.aspx. Last accessed 4th of July 2011.

National General Practitioner Information Technology Group. (2009). Scanning and

Shredding Documents: Impact Statement. http://www.icgp.ie/go/in_the_practice/information_technology/publications_reports. Last accessed 7th of July 2011.

National Institute of Health Enterprise Architecture. (2008). What is enterprise architecture?. Available: http://enterprisearchitecture.nih.gov/About/What/. Last accessed 7th of July 2011.

National Security Agency. (2011). Best Practices for Keeping Your Home Network Secure. Available: http://www.nsa.gov/ia/_files/factsheets/Best_Practices_Datasheets.pdf. Last accessed 7th of July 2011.

NIST, the National Institute of Standards and Technology. (2001). Announcing the ADVANCED ENCRYPTION STANDARD (AES). Available: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf. Last accessed 4th of July 2011.

North Atlantic Treaty Organisation. (2011). Probable data breach from a NATO-related website. Available: http://www.nato.int/cps/en/natolive/news_75729.htm. Last accessed 20th of June, 2011.

NSA. (2000). *NSA/CSS STORAGE DEVICE DECLASSIFICATION MANUAL.* Available: http://www.nsa.gov/ia/_files/government/MDG/NSA_CSS_Storage_Device_Declassification_Manual.pdf. Last accessed 4th of July 2011.

Oates, J. (2011). (A). Has UK gov lost the census to Lulzsec?. Available: http://www.theregister.co.uk/2011/06/21/uk_census_lost/. Last accessed 10th of July 2011.

Oates, J. (2011). (B). NHS bitchslapped by ICO on data security. Available: http://www.theregister.co.uk/2011/07/01/nhs_data_failure/. Last accessed 10th of July 2011.

Oda, S.M.; Huirong Fu; Ye Zhu; , "Enterprise information security architecture a

review of frameworks, methodology, and case studies," Computer Science and Information Technology, 2009. ICCSIT 2009. 2nd IEEE International Conference on , vol., no., pp.333-337, 8-11 Aug. 2009. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5234695&isnumber=5234374. Last accessed 7th of July 2011.

OWASP Guide Project. (2011). The Open Web Application Security Project (OWASP). Available: https://www.owasp.org/index.php/OWASP_Guide_Project. Last accessed 4th of July 2011.

Payne, S. (2006). A Guide to Security Metric. Available: http://www.sans.org/reading_room/whitepapers/auditing/guide-security-metrics_55. Last accessed 10th fo July 2011.

Peterson, G. (2007). Security Architecture Blueprint. Available: http://arctecgroup.net/pdf/ArctecSecurityArchitectureBlueprint.pdf. Last accessed 7th of July 2011.

Rigney C, Willens S, Livingston, Rubens A, Merit, Simpson W, Daydreamer. (2000). Remote Authentication Dial In User Service (RADIUS). Available: http://www.ietf.org/rfc/rfc2865.txt. Last accessed 4th of July 2011.

Room S. (2008). Using ISO 27000 to comply with Data Protection Act principles. Available: http://searchsecurity.techtarget.co.uk/tip/Using-ISO-27000-to-comply-with-Data-Protection-Act-principles?ShortReg=1&mboxConv=searchSecurityUK_RegActivate_Submit&. Last accessed 28th of March 2011.

SANS Institute. (2005). Design Secure Network Segmentation Approach. Available: http://www.sans.org/reading_room/whitepapers/hsoffice/design-secure-network-segmentation-approach_1645. Last accessed 4th of July 2011.

Savage, M. (2009). NHS 'loses' thousands of medical records. Available: http://www.independent.co.uk/news/uk/politics/nhs-loses-thousands-of-medical-

records-1690398.html. Last accessed 8th January 2011.

Scarfone et al, (2008, C), Scarfone K, Souppaya M, Cody A and Orebaugh A. (2008). Technical Guide to Information Security Testing and Assessment. Available: http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf. Last accessed 4th of July 2011.

Scarfone K and Hoffman P. (2009). Guidelines on Firewalls and Firewall Polic. Available: http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf. Last accessed 4th of July 2011.

Scarfone K, Jansen W, Tracy M. (2001). Guide to General Server Security. Available: http://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf. Last accessed 4th of July 2011.

Scarfone K, Souppaya M and Johnson P. (2008). (A). Guide to Securing Microsoft Windows XP Systems for IT Professionals- A NIST Security Configuration Checklist. Available: http://csrc.nist.gov/itsec/SP800-68r1.pdf. Last accessed 4th of July 2011.

Stoneburner, Garry. (2001). Underlying Technical Models for Information Technology Security. Available: http://csrc.nist.gov/publications/nistpubs/800-33/sp800-33.pdf. Last accessed 7th of June, 2011.

Shafer, M. (2010). Cisco for Small Business – An Example Network Case Study. Available: http://www.shaferconsulting.com/2010-cisco-for-small-business-an-example-network-case-study. Last accessed 15th fo July 2011.

The Australian Computer Emergency Response Team (AusCERT) and the CERT® Coordination Center (CERT/CC). (2001). UNIX Security Checklist v2.0. Available: http://www.rigacci.org/docs/biblio/online/usc20/usc20_full2.html. Last accessed 4th of July 2011.

The Data Protection Commissioner. (2011). *REGISTRATION CLASSIFICATION & GUIDANCE NOTES FOR APPLICATION*. Available:

http://www.dataprotection.ie/docs/Registration_Classification_&_Guidance_notes_for_Applica/745.htm#pm. Last accessed 28th of March 2011.

The Irish College of General Practitioners and the National General Practice Information Technology Group. (2003). Managing and Protecting the privacy of Personal Health Information in Irish General Practice, An Information Guide to the Data Protection Acts for General Practitioners. Available: http://www.icgp.ie/go/in_the_practice/information_technology/publications_reports. Last accessed 6th of July 2011

The MITRE Corporation. (2006). Electronic Health Records Overview. Available: http://www.ncrr.nih.gov/publications/informatics/ehr.pdf. Last accessed 7th of July, 2011.

Tulu B and Chatterjee S. (2003). A new security framework for HIPAA compliant health information systems. In Ninth Americas Conference on Information Systems, (2003)

Tulu, B and Chatterjee, S. (2003). A new Security Framework for HIPAA Compliant Health Information Systems. Ninth Americas Conference on Information Systems. 929-938

Verser R. (1997). *DESCHALL Press Release.* Available: http://home.earthlink.net/~rcv007/despr4.htm. Last accessed 28th of March 2011

Vijayan, Jaikumar. (2010). Anonymous attack on Amazon.com appears to fail. Available: http://www.computerworld.com/s/article/9200639/Anonymous_attack_on_Amazon.com_appears_to_fail. Last accessed 7th of June, 2011

Wafa, T. (2010). How the Lack of Prescriptive Technical Granularity in HIPAA Has Compromised Patient Privacy. NORTHERN ILLINOIS UNIVERSITY LAW REVIEW. 30, 531-552.

Wakabayashi, D. (2008). Microsoft sees Windows gaining server market share. Available: http://www.reuters.com/article/2008/02/28/us-microsoft-servers-idUSN2748543820080228. Last accessed 27th June 2011

Walsh, Rick. (2010). Folk Models of Home Computer Security Symposium on Usable Privacy and Security (SOUPS). Available: http://cups.cs.cmu.edu/soups/2010/proceedings/a11_Walsh.pdf. Last accessed 7th of June, 2011.

APPENDIX A – DATA PROTECTION DEFINITIONS

"***Data*** *means information in a form which can be processed. It includes both automated data and manual data.*

Automated data *means, broadly speaking, any information on computer, or information recorded with the intention of putting it on computer.*

Manual data *means information that is kept as part of a relevant filing system, or with the intention that it should form part of a relevant filing system.*

Relevant filing system *means any set of information that, while not computerised, is structured by reference to individuals, or by reference to criteria relating to individuals, so that specific information is accessible.*

Personal data *means data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller. This can be a very wide definition depending on the circumstances.*

Processing *means performing any operation or set of operations on data, including: – obtaining, recording or keeping data,*

– collecting, organising, storing, altering or adapting the data, – retrieving, consulting or using the data,

– disclosing the information or data by transmitting, disseminating or otherwise making it available,

– aligning, combining, blocking, erasing or destroying the data. ***Data Subject*** *is an individual who is the subject of personal data.*

Data Controllers *are those who, either alone or with others, control the contents and use of personal data. Data Controllers can be either legal entities such as companies, Government Departments or voluntary organisations, or they can be individuals such as G.P.'s, pharmacists or sole traders.*

Data Processor *is a person who processes personal data on behalf of a data controller, but does not include an employee of a data controller who processes such data in the course of his/her employment. Again individuals such as G.P.'s, pharmacists or sole traders are considered to be legal entities.*

Sensitive personal data *relates to specific categories of data which are defined as data relating to a person's racial origin; political opinions or religious or other beliefs; physical or mental health; sexual life; criminal convictions or the alleged commission of an offence; trade union membership.*
You have additional rights in relation to the processing of any such data."

Data Protection Acts 1988 and 2003 A Guide For Data Controllers, (2011)

APPENDIX B – INTERVIEW QUESTIONS

Practice Background Information

Roughly, how many of the practice have for the following

Patients:

Doctors:

Nurses:

Other Staff:

Governance and procedural Questions

1. Is your practice registered as a data processor of health data?

2. Is there an internal data protection policy that is relevant to the personal data held?

3. Do you have a policy for who needs access to health information? (The Data Protection Commissioner stipulates that: *Access to any personal data within an organisation to be restricted to authorised staff on a 'need-to-know' basis in accordance with a defined policy*)?

    a. Can administrative staff access patient information to the same extent that medical staff can, including to modify it?

    b. If so, what is the need for this?

4. Is access to computer equipment password protected?

a. Including unlocking a screen? How long does it take for a screen to lock or is there a policy of staff automatically locking their screens when they are not in use?

b. Is there a centralised logon service for usernames and passwords?

c. Do users share usernames and passwords?

d. How to locum doctors get access to the data they need?

e. Is there a password change policy, including for when users leave

f. Are access restrictions applied to sensitive data, i.e. do you need a username and password to access any EHR/ HIS systems you have, are the passwords for that different from the passwords you use to log onto your computer?

g. Are global permissions used, i.e. by default all users get access to any and all information?

h. What is the procedure for when new staff joins for them to gain access to information

5. Is a designated person responsible for security and for periodic reviews of the measures and practices in place?

    a. If so, how often are those reviews carried out?

6. Physical Files:

    a. Do you have a shredder for sensitive printed materials or a similar mechanism?

    b. Is access to manual, physical records controlled?

    c. Are filing cabinets locked when not in use, how is access to the keys controlled?

7. Are staff members trained in security and data protection matters?

    a. Would staff be disciplined for data breaches? Is there a formalised procedure for such?

b. Have all persons in the practice (not already covered by a professional confidentiality code) signed a confidentiality agreement that explicitly makes clear their duties in relation to personal health information and the consequences of breaching that duty.

c. Are staff made aware of the importance of patient confidentiality so that patient information is never given out inappropriately especially over the phone?

8. Can you identify your Data Controller's?

    a. Are your data controllers aware of their requirements to keep data protected, including the technical requirements?

9. Who are your data processors?

10. Do you have a data retention policy? i.e. how long do you maintain records on users for.

    Do you have:

- A defined policy on retention periods for all items of personal data kept
- Management, clerical and computer procedures in place to implement such a policy.

11. Do you have a data subject access request process?

12. Do you have a data breach response plan?

    a. Have you ever suffered a data breach?

13. Is patient information ever included in email, including internally in the office?

    a. Is email a secure form of communication?

    b. Is it possible to do so, i.e. copy and paste?

    c. Can Health data be saved on a USB key?

14. Are you aware that the maximum fine for a data breach is €100,000?

15. Are you concerned about data protection matters for the practice?

    a. Would you be willing to invest more in data protection matters?

    b. Would you be willing to pay for such services?

    c. Would you be willing to become compliant with any standards, etc in the area?

16. Are you aware that the Health Information Bill proposed by the last government proposed greater use of health information and the need to secure and protect it?

Technical Questions

1. Who is responsible for the technical and IT side of the practice?

    a. Do they monitor for vulnerabilities, i.e. Windows patches on Patch Tuesday?

2. Do you have an EHR or HIS?

    a. If so, what is it?

    b. Is your EHR/ HIS security certified, for any of the following?

    - ISO27001 - ISO 27799:2008 Health informatics - Information security management in health using ISO/IEC 27002
    - Health Level 7, HL7
    - ISO/TS 21091:2005 Health informatics -- Directory services for security, communications and identification of professionals and patients
    - CEN 13606 - Health informatics - Electronic Health Record Communication (EN 13606) European Standard
    - ASTM E1869 - 04(2010) Standard Guide for Confidentiality, Privacy, Access, and Data Security Principles for Health Information Including Electronic Health Records
    - Any other similar standard

    c. What data is contained in it?

    d. Who is responsible for administering it?

e. If they are an external body is there any internal knowledge on the matter for audit purposes?

f. Is a secure form of communication such as SSL/ TLS employed between the server and the clients that access it?

3. What type of router, firewall is in place?

    a. Is it configured as per manufactures requirements and recommendations?

    b. Is it hardened with all unnecessary services disabled? E.g. IP source routing?

    c. Do you know what services and protocols your router will pass or can you easily access that information?

    d. Do you have medical devices that connect to the network?
        a. If so, what are they?
        b. Do they have a computer operating system
        c. What are they used for
        d. Is someone responsible for administering them
        e. Do they store or record any health data
        f. Do they directly process any identifiable health data

4. Do your computers connect to a wireless network?

    a. If so, can you access the HIS, HER or any other office system that can store or process health data from that wireless network?

    b. Is the wireless network encrypted and if so what level?
        a. Are other best practice wireless security procedures implemented

5. Do you store medical data in another location on the network other than a EHR/ HIS? E.g. letters and scanned documents on a file server, email, CRM, any kind of web database that collects data, say for booking appointments, etc.

    a. If so what access protections and encryption is in place if any?

    b. If so what type of data is retained, e.g. emails or records of letters?

c. Are any protections applied to the server/ workstation that stores the data?

d. Is any medical data stored on a webserver or a server that is running a web server process such as Apache or IIS

6. Is there a procedure for when a computer, server, laptop, etc or a hard drive or other storage device is replaced to destroy the contents of the hard drive?

7. Is your data backed up, if so how? Tape/ Disk/ Etc

    a. Is data backed up offsite? If so is it saved in an encrypted format?

    b. Have you tested your backup recovery capabilities?

    c. Is someone specifically responsible for backup's?

8. What OS do your client computers use?

    a. Do you used any standard for securing client workstations, e.g. the Guide to Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist

    b. How do your client computers receive operating system and other software updates? Are automatic updates enabled?

    c. Do users get administrative rights normally?

    d. Is there a centrally managed system for updates?

    e. Who monitors to ensure that your computers receive their updates?

    f. What Anti Virus Software is installed on them?

    g. Is it set to automatically update?

    h. Is it managed to ensure that it automatically updates?

i. Have you ever gotten a virus?

j. Do you use full disk encryption or any other type of encrytion on laptops or other portable devices?

k. Is medical and health data stored on individual workstations as opposed to a central location?

l. Is disk encryption used for laptops or storage media such as USB keys?

9. What OS do your server computers use? Including any servers that run you're his/ EHR

   a. Are your servers hardened as to best practices and supplier recommendations? If so, what standards or recommendations are used? E.g. Microsoft Exchange Server 2003 Security Hardening Guide[6]

   b. Do you have a security policy in place for your servers? If so what is it based on? E.g., SANS – Server Security Policy[7]. Also, SANS - information-security-policy-development-guide-large-small-companies_1331

   c. What OS level security technologies are in place?
      i. Data-execution protection (DEP)
      ii. Address-space layout randomization (ASLR)
      iii. Sandboxing
      iv. Code signing
      v. Application firewall
      vi. Does the files system on the server support file level security and encryption?

   d. Are the services a user can access on a server controlled? That is are Service Access Control Lists implemented or are all services globally available to all users?
      i. This is of particular interest for any HIS/ EHR software that is running

   e. Is the data stored on the server encrypted?

[6] http://www.microsoft.com/downloads/en/details.aspx?FamilyId=6A80711F-E5C9-4AEF-9A44-504DB09B9065&displaylang=en

[7] http://www.sans.org/security-resources/policies/Server_Security_Policy.pdf

f. Do your servers employ signed certificates for authentication, encryption, non repudiation, etc?

g. What physical access controls are in place for access to servers?

h. Patching policy for server and client software?
    i. Whose responsibility is this?

i. Is RAID or another form of disk redundancy used?

j. Are your servers connected to a specific server network or do they implement their own firewall's to replicate such a state?

10. Do you have a remote access policy? For both staff and contractors?

    a. Can data be accessed from a remote site, e.g. VPN? If so how and what security measures are in place?

    b. Can third party contractors access your medical data? If so, how and when? Is there a formal agreement in place to monitor, request and control that? Who is responsible for those controls?

    c. Are VPN's, either SSL or IPSEC used for this?

11. Do you have a means for detecting and preventing data breach's or security incidents? E.g. an IDS

12. Are there any "Cloud" or online, internet hosted third party services used where medical information could be stored, e.g. online backups or other file storage services?

APPENDIX C – CORRESPONDENCE WITH THE SECURITY EXPERT ON THE MODEL

Correspondence 1, from Security Expert

Hi Sean,

I had a look at it again last night and I guess I still have the same thoughts/recommendations as before, but also one or two more ideas to consider. Below are my main points from last time and from looking again last night.

1. Inside, outside, over differentiation

- Systems or states
- I think maybe it could be made clearer that for example data can be in the 'over' state while at the same time a system can be an 'over' system if it helps data to be in the 'over' state.

2. Another very useful set of hardening standards are the cis guidelines. We make use of these regularly. They are very good and cover many platforms.

- www.cisecurity.org

3. Possibly rework the overall model to:
A. Start with a type of thing to be secured
B. Then go down the state
... easier to actually implement the model
e.g. Step 1 – We have some data. Step 2 – We want to protect it while in the 'over' state. Step 3 – Move down to the specific configuration steps for 'data' in the 'over' state. Step 4 – Move down to any relevant standards for this 'data' in the 'over' state.

4. Always look at it from the perspective of a person who is implementing it and see how they would work their way through the model to get the outcome that they should get.

5. Consider solidifying the actual final steps to implement the standard. The two main standards that we use are ISO27001 and PCI. The reason I personally prefer PCI is that the person implementing it is given more solid steps to actually get into compliance with it. ISO is more vague and so therefore difficult to know whether you are actually in compliance. For a masters thesis I'm sure you wouldn't be expected to have all the scenarios nailed but you could potentially have a mention that a fuller release version of the model would go in that direction ... If you agreed with me of course! J

6. What has to be done rather than what could be done ...
- People must follow what it says in order to comply
- From reading at a couple of parts it feels like you are giving some recommendations whereas if you are looking at this as a security model that people can become compliant with, implementation steps should be worded as though you are demanding that this be done. E.g. ISO uses the word 'shall' a lot. The word must is similar. Basically if you don't do this you are not compliant, not just well you can do this if you feel like it. It should be a minimum set of requirements that they must fill in as a base. They can go over as much as they want but they will not be considered as compliant unless they reach a certain point that you specify.

7. Similarity to PCI in that the main goal is protection of one thing ... PHI. In PCI that one thing is Credit Card Information. Therefore you could possibly take some ideas from PCI in this regard. E.g.
- In order to comply with the standard, a defined scope is needed. This will include any area of the network that transmits, processes or stores PHI information (ref. Inside, outside or over state). Any area within this scope must follow the standard fully, otherwise it is not in compliance. Any area that is not in scope must be provably so. This could be for example a separate wireless network that the medical practice run in their waiting room. There should be no link to any servers and no possibly way of penetrating through to these.
- Regularly monitor and test networks.
- Etc. Check out the 'Control Objectives' of PCI for an overview. The Wikipedia has a brief summary.

I hope this helps.

I can call you at lunch time or after work today if you like.

Regards,
Darren Fitzpatrick
Information Risk and Compliance Consultant

Correspondence 2, Authors Follow up

That’s great Darren, sorry I didn't get back to you yesterday but you know how it is. The feedback you have sent is really useful.

For point 3 below, a way of re-working the model. I think what you describe is actually what I am trying to achieve, i.e. you have this PHI to protect, it can be in several 'states' so you look at each state and then take action on each to protect the PHI, those actions could also be categorized down further. So I suspect we are signing off the same hymn-sheet. It may be more likely that the way I expressed this idea is confusing and that needs some re-work, so I will try to do that.

Also the way of looking at it from the perspective of who will be applying it is really important too, I don't think I will be able to do much to re-workl the model from that direction with the short time frame but I am going to mention that you said that in the dissertation document. The same for solidifying the actual steps and making them more concrete, that too is great advise and I wish I hadn't left it so late to get it from you.

Would you be happy to describe the model as valid? I.e. that it is an effective way of securing PHI in small medical practices, with or without your changes?

Correspondence 3, Security expert’s subsequent response

No problem Sean.

Yes, if we had more time we probably could have worked together some more, but it is looking good anyway. Thinking back to my masters too I would think that you bringing me on-board will sound pretty good and hopefully it helped a little. From the looks of things I'd say you will do well.

Given the guidance provide using the concepts of systems and services classifications, their relevant security measures and resources and the 'state' in which data is secured, I would be happy to describe the model as valid. The model, in its current state seems conceptually sound as the foundations of a usable security model for PHI in small medical practices.

APPENDIX D - INTERVIEW ANALYSIS, ALL QUESTIONS

		Practice Number				
	Question Details	**1**	**2**	**3**	**4**	
Data Protection and Governance						
Question						**Question classification**
1	Registration	adq	adq	adq		1
2	DP Policy	not	not	adq	adq	1
3	PHI Access Policy	not	not	adq	adq	1
3a	Admin staff	not	not	adq	adq	1
3b	Need for staff	adq	some	adq	adq	1
4	Password Protected	adq	adq	adq	adq	2
4a	Screen lock	some	some	some	adq	2
4b	Directory Service	adq	adq	adq	adq	2
4c	logon sharing	some	some	adq	adq	2
4d	locums	adq	some	adq	adq	1
4e	password changes	adq	not	adq	adq	2
4f	sesnitive data restricted	some	adq	adq	adq	2
4g	global perms	not	not	adq		2
4h	new staff policy	adq	adq	adq	adq	2
5	person check security	some	some	adq		1
5a	review period	not	not	some		1
6a	shredder	adq	adq	adq	adq	3
6b	access to files	adq	adq	adq		3
6c	locked cabinet	some	adq	adq		3
7	security training	some	some	some	adq	4
7a	staff disciplined?	adq	adq	adq	adq	4
7b	contracts	adq	adq	adq	adq	4
7c	staff awareness	adq	adq	adq	adq	4
8	id controllers	not	some	not	adq	4
8a	controller awareness	some	adq	not	adq	4
9	processors	some	adq		adq	4
10	data retention	adq	some	some	adq	1
10a	periods	some	not	some	adq	1
10b	procedures for retention	not	not	not	adq	1
11	subject access req	some	some	adq	adq	1
12	data breach response	not	not	adq	adq	1
12a	sufferred a data breach	not	not	adq		1
13	PHI in email	adq	adq	adq	adq	2
13a	is email secure	not	adq	adq	adq	4
13b	copy and paste	adq	some	some	not	2
13c	PHI on usb	adq	some	some	adq	2

14	max fine	not	not	adq	adq		4
15	concerned about dp	not	adq	adq			4
15a	willing to invest	not	not	not			4
15b	pay for such	not	not	not			4
15c	willing to become compliant	some	adq	adq			4
16	HIB awareness	not	adq	adq			4
Technical Questions							
1	who responsible for IT	adq	some	adq			5
1a	vuln monitoring	not	some	some			5
2	HIS?	adq	adq	adq	adq		6
2a	what HIS						6
2b	HIS security certified	not	not	adq	adq		6
2c	data in HIS?	adq	adq	adq	adq		6
2d	who is responsible for HIS	adq	adq	adq	adq		6
2e	internal knowledge of HIS	not	not	some	not		6
2f	secure comms HIS	some	not	adq	adq	6\8	
3	Router/ Firewall	adq	adq	adq	adq		8
3a	configured properly	adq	adq	adq	adq		8
3b	hardened	adq	adq	adq	adq		8
3c	id services?	not	not		adq		8
3d	medical devices	some	some	adq	adq		7
4	wireless	adq	adq	adq	adq		8
4a	access HIS from wlan	adq	adq	adq	adq		8
4b	wireless encrypted	adq	adq	adq	adq		8
4ba	other wlan sec configs	some	adq	adq	adq		8
5	store PHI outside HIS	adq	adq	adq	adq		7
5a	protection	adq	adq	adq	adq		7
5b	type of data	adq	adq	adq	adq		7
5c	protection to host	adq	adq	adq	adq		7
5d	PHI on webserver	adq	adq	adq	adq		7
6	data destruction	adq	adq	adq	adq		7
7	backups	adq	adq	adq	adq	7\8	
7a	offsite	some	some	adq	adq		7
7b	tested	adq	adq	adq	adq		7
7c	person responsible	adq	adq	adq			7
8	client os	some	some	some	some		7
8a	os sec config templates	adq	not	some			7
8b	os patches	not	adq	some			7
8c	user admin rights	adq	adq	adq			7
8d	central managed updates	not	some	some			7
8e	who monitors updates	not	some	some			7
8f	AV	adq	adq	adq			7
8g	av updates	adq	adq	adq			7
8h	av managed	adq	some				7
8i	got a virus	adq	adq	adq			7
8j	disk encryption for portables	adq	adq	adq		7\8	

8k	PHI on workstations	adq	adq	adq			7
8l	laptop encryption	some	adq	adq		7\8	
9	server os	some	adq	some	adq		7
9a	server hardening	adq	some	adq	adq		7
9b	server security policy	adq	not	adq	adq		7
9c	os security mechanisms				adq		7
9d	sacls				adq		7
9e	server encrypted	not	not		not		7
9f	certs						7
9g	physical access controls	adq	adq	adq	adq		7
9h	server patching	adq	adq	adq	adq		7
9i	RAID	adq	adq	adq			7
9j	server vlan	adq	not	not			8
10	VPN policy	adq	adq	adq	adq		8
10a	access PHI from VPN	adq	some	adq	adq		8
10b	contractors access	adq	not	adq			5
10c	sec measures	adq					7
11	IDS	adq	not	not			8
12	Cloud	adq	adq	adq			7

Key
not = Not adequate
some = Somewhat adequate
adq = Adequate

Classification of interview questions

1: documented procedural protections and policy compliance
2: account & PHI access controls
3: physical files
4: Staff training and control matters
5: Assigned responsibilities for security matters
6: Inside
7: Outside
8: Over

APPENDIX F - AGGREGATED RESULTS BY CLASSIFICATION OF INTERVIEW QUESTION

1: Documented procedural protections and policy's

ADQ = 9 SOME = 1 NOT = 4

2: Account & PHI access controls

ADQ = 7 SOME = 3 NOT = 1

3: Physical files

ADQ = 0 SOME = 3 NOT = 0

4: Staff training and control matters

ADQ = 4 SOME = 6 NOT = 4

5: Assigned responsibilities for security matters

ADQ = 1 SOME = 0 NOT = 1

6: Inside

ADQ = 3 SOME = 1 NOT = 1

7: Outside

ADQ = 25 SOME = 7 NOT = 1

8: Over

ADQ = 7 SOME = 0 NOT = 2

ADQ = 1 SOME = 0 NOT = 0

Combination Classifications

					access PHI from	
6\8	adq	some	adq	adq	VPN	adq
7\8	adq	not	adq		contractors access	adq
7\8	adq				sec measures	
7\8	adq	not	not		IDS	not
	adq	adq	adq		Cloud	adq

Key

not = Not adequate
some = Somewhat adequate
adq = Adequate

Classification of interview questions

1: documented procedural protections and policy compliance
2: account & PHI access controls
3: physical files
4: Staff training and control matters
5: Assigned responsibilities for security matters
6: Inside
7: Outside
8: Over

APPENDIX E – FINDINGS BY CLASSIFICATION FOR INDIVIDUAL PRACTICE

Practice 1
1: Documented procedural protections and policy's
ADQ = 7 SOME = 3 NOT = 4 N/A = 0
2: Account & PHI access controls
ADQ = 5 SOME = 4 NOT = 2 N/A = 0
3: Physical files
ADQ = 1 SOME = 2 NOT = 0 N/A = 0
4: Staff training and control matters
ADQ = 4 SOME = 2 NOT = 7 N/A = 0
5: Assigned responsibilities for security matters
ADQ = 2 SOME = 0 NOT = 1 N/A = 0
6: Inside
ADQ = 3 SOME = 0 NOT = 2 N/A = 1
7: Outside
ADQ = 23 SOME = 6 NOT = 3 N/A = 1
8: Over
ADQ = 7 SOME = 1 NOT = 1 N/A = 3

Practice 2
1: Documented procedural protections and policy's
ADQ = 5 SOME = 4 NOT = 5 N/A = 0
2: Account & PHI access controls
ADQ = 8 SOME = 3 NOT = 1 N/A = 0
3: Physical files
ADQ = 1 SOME = 1 NOT = 1 N/A = 0
4: Staff training and control matters
ADQ = 5 SOME = 3 NOT = 6 N/A = 0
5: Assigned responsibilities for security matters
ADQ = 0 SOME = 2 NOT = 0 N/A = 1
6: Inside
ADQ = 3 SOME = 0 NOT = 2 N/A = 1
7: Outside
ADQ = 24 SOME = 6 NOT = 3 N/A = 0
8: Over
ADQ = 5 SOME = 1 NOT = 3 N/A = 3

Practice 3
1: Documented procedural protections and policy's

ADQ = 13 SOME = 1 NOT = 0 N/A = 0

2: Account & PHI access controls

ADQ = 7 SOME = 2 NOT = 2 N/A = 0

3: Physical files

ADQ = 0 SOME = 2 NOT = 0 N/A = 0

4: Staff training and control matters

ADQ = 9 SOME = 2 NOT = 3 N/A = 0

5: Assigned responsibilities for security matters

ADQ = 1 SOME = 1 NOT = 0 N/A = 0

6: Inside

ADQ = 4 SOME = 1 NOT = 0 N/A = 1

7: Outside

ADQ = 26 SOME = 4 NOT = 0 N/A = 2

8: Over

ADQ = 6 SOME = 1 NOT = 1 N/A = 4

Practice 4

1: Documented procedural protections and policy's

ADQ = 12 SOME = 0 NOT = 0 N/A = 2

2: Account & PHI access controls

ADQ = 7 SOME = 0 NOT = 0 N/A = 4

3: Physical files

ADQ = 3 SOME = 0 NOT = 0 N/A = 0

4: Staff training and control matters

ADQ = 7 SOME = 0 NOT = 1 N/A = 6

5: Assigned responsibilities for security matters

ADQ = 0 SOME = 0 NOT = 0 N/A = 2

6: Inside

ADQ = 4 SOME = 0 NOT = 1 N/A = 1

7: Outside

ADQ = 19 SOME = 1 NOT = 0 N/A = 13

8: Over

ADQ = 8 SOME = 0 NOT = 1 N/A = 3

Key

not = Not adequate
some = Somewhat adequate
adq = Adequate